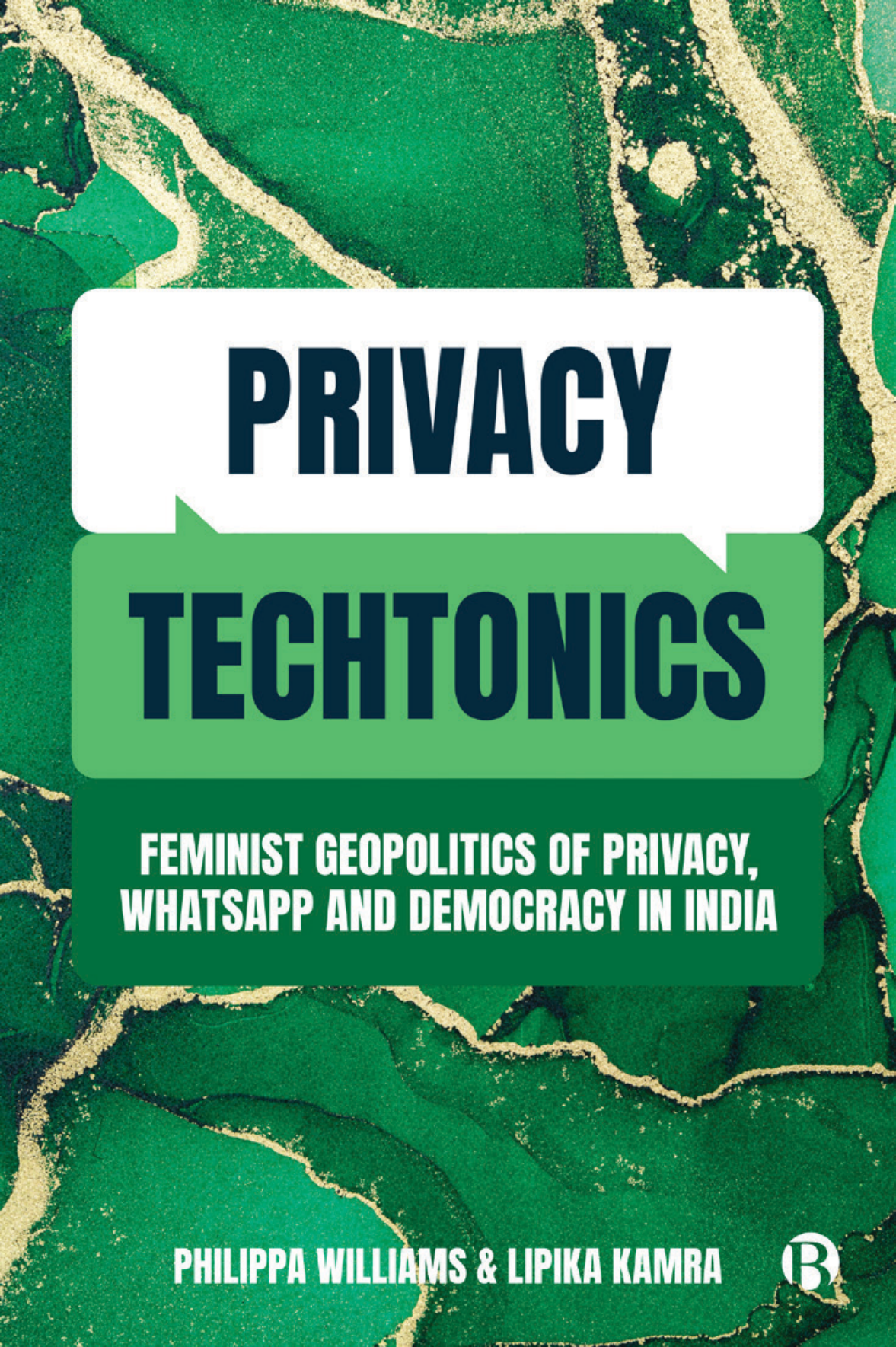




PRIVACY TECHTONICS

**FEMINIST GEOPOLITICS OF PRIVACY,
WHATSAPP AND DEMOCRACY IN INDIA**

PHILIPPA WILLIAMS & LIPIKA KAMRA



PRIVACY TECHTONICS

Feminist Geopolitics of Privacy, WhatsApp
and Democracy in India

Philippa Williams and Lipika Kamra



First published in Great Britain in 2026 by

Bristol University Press
University of Bristol
1-9 Old Park Hill
Bristol
BS2 8BB
UK
t: +44 (0)117 374 6645
e: bup-info@bristol.ac.uk

Details of international sales and distribution partners are available at bristoluniversitypress.co.uk

© Philippa Williams and Lipika Kamra 2026

DOI: [10.51952/9781529235982](https://doi.org/10.51952/9781529235982)

The digital PDF and ePub versions of this title are available open access and distributed under the terms of the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International licence (<https://creativecommons.org/licenses/by-nc-nd/4.0/>) which permits reproduction and distribution for non-commercial use without further permission provided the original work is attributed.

British Library Cataloguing in Publication Data

A catalogue record for this book is available from the British Library

ISBN 978-1-5292-3596-8 paperback

ISBN 978-1-5292-3597-5 ePub

ISBN 978-1-5292-3598-2 OA PDF

The right of Philippa Williams and Lipika Kamra to be identified as authors of this work has been asserted by them in accordance with the Copyright, Designs and Patents Act 1988.

All rights reserved: no part of this publication may be reproduced, stored in a retrieval system, used to train or develop an artificial intelligence system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise without the prior permission of Bristol University Press.

Every reasonable effort has been made to obtain permission to reproduce copyrighted material. If, however, anyone knows of an oversight, please contact the publisher.

The statements and opinions contained within this publication are solely those of the authors and not of the University of Bristol or Bristol University Press. The University of Bristol and Bristol University Press disclaim responsibility for any injury to persons or property resulting from any material published in this publication.

Bristol University Press works to counter discrimination on grounds of gender, race, disability, age and sexuality.

Cover design: Liam Roberts Design

Front cover image: 123rf/pitinan

Bristol University Press uses environmentally responsible print partners.
Printed and bound in Great Britain by CPI Group (UK) Ltd, Croydon,
CR0 4YY

Bristol University Press' authorised representative in the European Union is:
Easy Access System Europe, Mustamäe tee 50, 10621 Tallinn, Estonia,
Email: gpsr.requests@easproject.com



To James, Xan and Caspar

To my mother, Neeta

Contents

About the Authors	vi
Acknowledgements	vii
1 ‘The Future Is Private’	1
2 WhatsApp? Why India?	7
3 Privacy Techtonics	30
4 The Politics of Digital Private Messaging	59
5 Privacy and the Law	86
6 Privacy-by-design	122
7 Privacy Is (Geo)political	149
8 WhatsApp (in) Business	177
9 Conclusion	204
Appendix: Methodology	208
Bibliography	212
Index	244

About the Authors

Philippa Williams

Professor of Geography, Department of Geography, School of Society and Environment, Queen Mary University of London, UK

Philippa is a feminist political geographer whose research and teaching at Queen Mary University of London is animated through everyday political, digital and economic life. She explores how the state is experienced, how democracy is articulated, and how marginality – particularly in relation to violence and nonviolence – is lived. As well as publishing in international journals and media she has authored and co-edited books on *Everyday Peace*, *Geographies of Peace* and *Ordinary Work*. Philippa's focus on geopolitics of digital privacy, WhatsApp and democracy in India is her latest project. She was awarded the Philip Leverhulme Prize in Geography (2019–2022).

Lipika Kamra

Assistant Professor of Politics, Department of Political Science and International Studies, School of Government, University of Birmingham, UK

Lipika is a political anthropologist whose research and teaching interests lie at the intersection of state, democracy and digital politics. She studies how states and their citizens interact in insurgency and counterinsurgency contexts; how women mediate the terrain of development and democracy in India; and how digital media shapes everyday political life. She has published in international journals and media and is the author of the forthcoming book *Remaking the State: Women, Development and Counterinsurgency in India*.

Acknowledgements

This book is a collaborative effort that reflects the intellectual insights and challenge, generosity and support of numerous people who were formally and informally pulled into our book's orbit. The project began serendipitously in 2018 and has evolved in unexpected and compelling ways since then as we could not resist following the shifting contours of WhatsApp, privacy and democracy in India. Initial funding from WhatsApp (more on that in the book) and Philippa's Philip Leverhulme Prize from the Leverhulme Trust made researching and writing this book possible. We are grateful to both, for the funding and editorial freedom. Thanks to funding from Open Research Services at Queen Mary University of London's Library and Archives this book is Open Access. Finally, impact funding from Queen Mary created the chance to collaborate with curator Candice Jacobs on 'Privacy Techtonics' – an art exhibition on data privacy, power and people at Nottingham's Broadway gallery in 2022.

Most of the interviews for this book are thanks to excellent research assistance by Ekta Oza, Fatima Matin Khan, Mukesh Kumar, Pushpendra Johar, Shruti Arora and Zaheeb Ajmal with whom we have been lucky enough to work. We are grateful for these relationships and to those who shared their experiences and insights and on which basis we have formulated the book's arguments. Chapter 4 draws on paragraphs from earlier publications: Williams et al's (2022) No room for dissent: domesticating WhatsApp, digital private spaces, and lived democracy in India (*Antipode*, 54(1), 305–330), Kamra, Williams and Johar's (2023) Grassroots Authoritarianism: WhatsApp, middle-class boundary-making and pandemic governance in New Delhi's neighbourhoods (*Territory, Politics, Governance*, 6, 1121–1140) and Oza, Williams and Kamra's (2024) Digital denizenship: Hindu nationalist architectures of digital closings and unbelonging in India (*Environment and Planning C: Politics and Space*, 42(7), 1150–1169).

We are fortunate to work within supportive academic institutions and alongside some brilliant colleagues who have facilitated this book in different ways. Philippa is thankful to the Department of Geography in the School of Society and Environment at Queen Mary University of London. Lipika wishes to acknowledge the School of Liberal Arts and Humanities at O. P.

Jindal Global University, School of Politics and International Relations, School of Society and Environment at Queen Mary University of London, and the School of Government at the University of Birmingham. We would both also like to thank the Akademie Schloss Solitude where the book's outline was revised.

Our networks, relationships and inspirations extend beyond the institution and formal collaborations. We are both so appreciative of the support and challenge this book and our ideas have received from academic colleagues, friends and mentors in India and the UK who have given us a platform through seminars and conferences, as well as shared references, arguments, suggestions and time to read and engage with chapter drafts. These interactions were particularly valuable for developing and helping us to believe in the book's contribution. All errors and omissions are our own.

We are extremely grateful to Paul Stevens, the Senior Commissioning editor at BUP, for raising the expectations for what this book might be and are reassured to know it is the book you had hoped for. And to Ellen Mitchell for clarity and care in managing the production process, thank you. Our thanks also to three reviewers who sharpened the scope of the book at proposal stage and to two anonymous reviewers whose insightful suggestions helped refine the final manuscript.

Finally, to our closest family and friends, you know who you are: we could not have written this book without your welcome distractions, nourishing support and unconditional love. Thank you.

‘The Future Is Private’

Sabeena was in her early twenties and had recently completed a master’s in social work from Jamia Milia University, a public university in New Delhi with places historically reserved for Muslim students. She first downloaded WhatsApp in 2014 when smartphones ‘were recently launched’ in India and WhatsApp was installed ‘by everyone’, as she explained, it was an ‘exciting thing ... It was cool then. Everybody was using it; my friends were using it ... It was the in-thing.’ Though the excitement around smartphones and the novelty of WhatsApp had faded for her, WhatsApp was a fundamental, seemingly irreplaceable, inescapable part of every day. WhatsApp was the medium through which Sabeena’s family were in touch, where she received her daily news as well updates on college events and now work. Frustrated by the overwhelm of information on WhatsApp groups, her previous efforts to remove the app had inevitably resulted in her reinstalling the green icon. Removing WhatsApp was to remove yourself from life itself.

But on the other hand, Sabeena’s experience expressed the limits of privacy at the intersection of a private tech corporation, the Indian government and user-citizens. In 2019 the Indian government violently responded to students protesting against its amendment to the Citizenship Act which newly discriminated against Indian Muslims. Sabeena knew some of the students who were beaten and arrested by the police and worried that her association with them could make her a target of government surveillance too. As the conversation continued, she explained how ‘that entire scenario was pretty triggering and violating’:

Student phones are being tapped. You never know whether Facebook is sharing information with the government, and they own WhatsApp too. So, you don’t know when they [Facebook] might start sharing this information as well. So, whenever we discuss [things over WhatsApp] we say: ‘we shouldn’t be saying this since the call might be recorded’. So many people have been recorded on false charges [by the Indian government]. And if so many arrests can take place over a thing written

on Facebook or Instagram then how far is WhatsApp [safe] since it's also owned by Facebook? So, we don't say anything too controversial. We only share something that is already there.

On the one hand WhatsApp afforded Sabeena an intimate, immediate place of connection and care with her friends during particularly troubling times. Yet, despite knowing that WhatsApp's messaging was end-to-end encrypted, Sabeena was sceptical about how private her conversations with friends were. News headlines about Big Tech, Cambridge Analytica, and their use of personal data underscored her assumption that Facebook routinely shared information with the government, but moreover, as she put it 'the makers of the apps are not Indians' and can make up their own laws. And as for the government, led by the Bharatiya Janata Party for a third successive term, Sabeena was mistrustful. She had grown up in a progressively right-wing Hindu nationalist state that profiled her fellow Muslim students as national security threats and politically profited from the circulation of online hate and state violence targeted against people like her.

Prompted by critiques of India's new biometric data base, Aadhaar, in 2017 India's Supreme Court had pronounced that privacy *was* 'a distinct and independent fundamental right under Article 21 of the Constitution' which was enforceable and multifaceted. Privacy, and particularly with respect to digital technologies, had become a public matter in India. Yet, while the court ruling enshrined the legal right to privacy, its implications with respect to data protection had yet to be fully codified through national regulation, prompting calls for India's own form of GDPR, Europe's General Data Protection Regulation. But in any case, maintaining the privacy of her most private messages was near impossible should her or a contact's smartphone be seized by the police and her WhatsApp messages used as evidence to incriminate her. Sabeena's reflections surface her anxieties about the surveillance of India's minority Muslim community as well as the embeddedness of WhatsApp as a digital utility and the mundane privacy work that she and her friends habitually enacted when deciding what to share or not, in their digitally networked private spaces. While encryption infrastructure might make a digital space *technically* secure, the situated context and quality of digital private spaces matters more in Sabeena's everyday life.

If we trace a line from Sabeena's experience as a student in New Delhi to the 2019 Facebook F8! Developer conference hosted in San Jose, California, just a year earlier, the promise of digital private spaces looks very different. At this conference and in his accompanying blog, Mark Zuckerberg, the CEO of then Facebook (now Meta), declared that 'the future is private'. This announcement marked a discursive and technical shift in Meta's corporate vision, one that informs the transformation and fortunes of the company today. Zuckerberg's privacy pivot reorientated Facebook's focus away from

the ‘digital equivalent of the town square’ as a public space of sharing and connection to more private digital spaces characterized by ‘the digital living room’ occupied by Sabeena and her friends. WhatsApp, one of Facebook’s ‘family of apps’ with end-to-end encrypted messaging by default, was pitched as the paradigmatic case for realizing a private future. In an uncertain world Zuckerberg optimistically imagined that ‘over time I believe that a private social platform will be even more important in our lives than our digital town squares’ (Meta Developers, 2019, p 23). Witnessing Sabeena’s experience alongside Zuckberg’s pitch prompts us to question how a private social platform should become ‘even more important’ and whose interests would it serve?

The benefits of greater digital privacy would be hard to dispute, after all privacy is normatively agreed to be a *good* thing. Yet, particularly given the timing of the announcement, we might offer a cynical reading of Zuckerberg’s speculation on digital private messaging as a strategic response to the tech giant’s trouble with ‘public’ data and the fallout from Cambridge Analytica, lawsuits, US Congressional hearings on privacy, antitrust and misinformation, and user backlash. In other words, the ‘techlash’. Zuckerberg performatively acknowledged that interpretation too. Pausing, smiling to his audience of investors, developers and entrepreneurs he delivered a carefully scripted moment of self-reflection: ‘Now look, [laughing] I get that a lot of people aren’t sure that we’re serious about this. I know that we don’t have the strongest reputation on privacy right now, to put it lightly. But I’m committed to doing this well, and to starting a new chapter for our product.’ Acknowledging how much hard work this shift would require and how long it would take, Zuckerberg underlined his commitment to this future, explaining that ‘we’re also building out a lot of deep technical infrastructure and replumbing the whole infrastructure that we build for this company, to support this privacy vision’ (Meta Developers, 2019).

Against the backdrop of this privacy shift, *Privacy Techtonics* examines the global intimate relationship between privacy, private power and technology. When one of the world’s techno-oligarchs decides to replumb ‘the whole infrastructure’ of his company, we enquire into what happens when that future becomes the present, and now too the past? Whose future and whose private digital life did Zuckerberg imagine? What are the everyday implications of this ‘privacy vision’ for Sabeena, for Meta, WhatsApp, and the Indian government, among others? Like Elwood and Leszczynski (2011) and Igo (2018) we are far less concerned with defining what privacy is or should be but instead make privacy *the subject* by interrogating the stories that citizens, states and Big Tech tell themselves and us about privacy and digital private spaces. And, understood in context, we ask what do these stories tell us about how privacy is discursively, technically and materially actualized? And, how is privacy and power (re)configured on and through

different spaces, bodies and technologies? Following longstanding feminist thought, including feminist technoscience, feminist geopolitics and digital geographies, we understand digital privacy not only as political but also geopolitical. That is, as an idea, a practice and a thing, privacy is infused with power relations, from the intimate interfaces and images of the smartphone and the code running digital applications, to the structure and branding of corporations, to corporate privacy policies, citizens' legal petitions, regulatory authorities and government policies as well as the (digital) spaces in and through which sociopolitical life plays out. We do not put privacy on a pedestal as a value necessarily to be protected but lay bare the intricate politics of privacy in our world.

Privacy Tectonics imagines privacy and the private within the ethos of 'planetary scale computation' that is transforming what governance and sovereignty might mean (Bratton, 2015, p 3). Ben Bratton proposes a speculative framework of 'The Stack' to imagine a 'computational totality' that comprises hardware and software technologies that 'align layer by layer' to form an 'accidental megastructure' (Bratton, 2015, pp 4–5). This conceptualization helps in formulating an appreciation of the internet as more than social media and the smartphone, instead drawing attention to the multiplicity of things, layers and actors that it assembles, and is assembled through. Planetary scale computation acts like a 'planetary skin' enveloping the planet, aimed at recording, measuring and facilitating human and non-human processes in the form of data (Bratton, 2015, p 87).

The predatory extraction and processing of more and more *and more* data in conditions of scarcity has intensified under conditions of 'digital' or 'techno-feudalism' (Meinrath et al, 2011; Durand, 2024; Varoufakis, 2024). With its origins in cyber punk fantasy Cédric Durand (2024) develops the concept of 'techno-feudalism' to capture an emerging reality in which digital technology companies act like modern feudal lords who dominate the terms of exchange in the economy. Techno-feudalism operates in tandem with 'digital colonialism' (Birhane, 2020) or 'data colonialism' whereby technology companies' relationship to data, users and territory echoes and extends historical colonial power inequalities (Thatcher, O'Sullivan and Mahmoudi, 2016; Couldry and Mejias, 2019). Key to our argument is that attaining and sustaining access to data is realized through countless data privacy violations, manipulations and encroachments which are *made* to look normal, benign and inevitable through discursive and material practices. How then does publicly speculating on a private social platform serve Meta's and WhatsApp's future? The anthropologist Laura Bear has noted that as a technology of capitalist imagination 'speculation is akin to practices of divination or "magic"' ... 'deployed to anticipate the future; to stimulate its emergence; and to control it' (Bear, 2020, pp 2, 8). 'For most firms, privacy isn't a high priority because it isn't profitable.' (Citron, 2022, p 1).

But, in a data economy where metadata is more valuable than the content of personal communications, we illustrate how privacy ‘magic’, ‘myths’, ‘misdirections’ and ‘metaphors’ can be important enabling tools for Big Tech to expand its power through data (Hoepman, 2021; Waldman, 2021). In this case, a *private* future is a metaphorical ‘tonic’ for Facebook’s fortunes in the face of the 2018–2019 techlash. As something which refreshes, restores or stimulates, we argue that privacy as ‘tonic’ promised to discursively and materially regenerate Facebook. Chapter 3 develops this framework and brings together existing scholarship at the intersection of feminist geopolitics, feminist technoscience and critical internet studies, surveillance and privacy studies and politics.

Drawing on multi-sited research in north India, we ground how the speculative private ‘future’ presents in everyday life to examine how it is domesticated and vernacularized and with what implications for public-private life and lived democracy. We examine how the ideas of privacy are lived, understood, ignored and embraced in the spaces people inhabit on and around WhatsApp. The ‘lived encryptions’ of WhatsApp, that is how the key technological affordance of WhatsApp, end-to-end encryption, is interpreted, navigated, undermined and imagined with different meanings in people’s use of WhatsApp are important to consider (Udupa and Wasserman, 2025, p 13). As a material and imagined place, WhatsApp’s end-to-end encrypted private messaging also has a subterranean quality (Bratton, 2015; Udupa, Gagliardone and Hervik, 2021). Messages, memes and movies flow between the networked ‘deep addresses’ of WhatsApp’s ‘digital living rooms’ and beneath the surface of public scrutiny (Bratton, 2015, p 64). We show in Chapter 4 how in these encrypted spaces lived democracy is transformed, as political actors, activity and accountability are anonymized while the scale and speed of circulation of misinformation and hate speech is only moderated by the friction (or lack of) between computer code and human behaviour. Bringing a feminist geopolitical and feminist technoscience approach to the abstract concept of ‘the Stack’ embraces situated experiences and complexities and opens up to the uneven, contingent and messy, incremental and interconnected realities of the internet. For instance, Zuckerberg’s metaphorical ‘digital living room’ might convey a form of corporate communicative power but in practice it is not (always) a place of sanctuary, security and safety for Sabeena, or others. Experiences of digital private places are always unevenly intersected by gender, religion, ability, caste, race, sexuality and/or geography.

Like plate tectonics, privacy technonics are most energetic and animated at the boundaries of data privacy and publicity. The boundaries of WhatsApp’s digital private spaces are produced through the privatization of digital space while digital private messaging play host to communicative boundary-making practices of including and excluding different groups. Within a historical

context of self-regulation, Big Tech companies might be described as ‘legal entrepreneurs’ (Cohen, 2019b). And their privacy policies understood as a socio-legal contract between the platform and user, where struggles over the meaning of privacy surface at ‘the edge of the law’, as we show through WhatsApp’s privacy policies in Chapter 5 (Jeffrey, 2019). The discursive struggles over privacy are animated by the materiality of WhatsApp’s privacy architecture, in particular end-to-end encryption, which determines the technical boundaries around what is kept secure or ‘private’ on the platform. How encryption is given meaning and visibility within different geopolitical contexts through WhatsApp’s campaigns and the implications of these is the subject of Chapter 6. Meanwhile, Chapter 7 explores how ‘privacy’ is perceived and experienced in north India. Here privacy ruptures, data leakage and privacy violations, within intimate global contexts, surface the lived and affective dimensions of privacy talk and privacy things and how these reverberate within sociodigital lives. Finally, Chapter 8 documents how the introduction of WhatsApp Business from 2018 realized Meta’s ambition to transform WhatsApp into what it calls a ‘meaningful’ profit-making business, in this case one built on the power of WhatsApp’s network effect and marked by a significant erosion of WhatsApp’s privacy promise.

Our enquiry attends to how WhatsApp and digital privacy are entangled in processes of techno-feudalism and data colonialism by paying particular attention to the situated geographies of WhatsApp and digital privacy and how the domestication of WhatsApp both reflects and (re)produces socio-spatial inequalities. Viewing Silicon Valley, USA from and through India shifts the dominant vantage point from which privacy and technology are more often conceptualized and knowledge produced (Chan, 2014; Arora, 2019a). This book builds on scholarship that disrupts universal ideas of both privacy and digital technology. The ‘digital peripheries’ of India and the global south are the central location of *Privacy Tectonics* and for constructing a feminist geopolitics of privacy.

WhatsApp? Why India?

The ‘origin story’ of an ordinary technology

Every digital technology has an origin story; this is the origin story of WhatsApp and of the book. Research on digital technology is often drawn to emerging and esoteric technologies, such as driverless cars, space exploration or robots; we are fascinated by the ordinariness of WhatsApp as an everyday digital technology. Digital messaging apps are the most frequently opened apps on phones and often an important medium for other sociodigital experiences. Our approach is sympathetic to Lee Vinsel and Andy Russel’s point that we should be more attentive to the banal, ordinary technologies that constitute our everyday lives, and a little less fixated on techno boosterism and ‘emerging technologies’ which have relatively little bearing on the lives of the majority of the world ([Vinsel and Russell, 2020](#)). WhatsApp has 3 billion monthly active users (MAUs) as of June 2024 and was *the* leading communication channel for global smartphone users in 2024 ([Ceci, 2024](#)). It has evolved from an app with humble and moral aspirations to one of Meta’s ‘family of products’ wielding corporate power and ‘super app’ ambitions. This book is about that transformation and how WhatsApp became an intimate and immediate part of our everyday private (and public) lives.

WhatsApp was founded in [2009](#) by two software infrastructure engineers, Jan Koum and Brian Acton. They met while working at Yahoo! and developed a shared cynicism for technologies driven by ad revenue, something Koum found ‘depressing’ as he once reflected ‘You don’t make anyone’s life better by making advertisements work better’ ([Olson, 2014a](#)). The initial seeds for WhatsApp germinated from Koum’s idea to capitalize on Apple’s new App store by making a product that would pull in contacts’ address books so that networked individuals could see each other’s status updates. For instance, alerting them that your battery was low, or you were at the gym, in essence volunteering a response to the question ‘what’s up?’

which inspired the product's name. Koum incorporated WhatsApp Inc. in California on 24 February 2009.

The original aim was always for WhatsApp to be an international app. Koum reportedly spent days and weeks meticulously finessing the code to ensure that WhatsApp worked seamlessly within and between countries and regions. But only a few thousand people downloaded it on their iPhones, causing Koum to doubt that it would ever take off. WhatsApp's fortunes shifted when Apple launched push notifications in June 2009 which enabled developers to 'ping users when they weren't using the app' (Olson, 2014a). Koum edited the app so that every time a user changed their status, all their network contacts received an update alert. With this edit, the app captivated people's imagination and encouraged the sharing of mundane, sometimes humorous updates like 'I woke up late' or 'I'm on my way' (Olson, 2014a). Parmy Olson has documented how these immediate updates soon morphed into a form of instant messaging with status eliciting responses from friends and family. Koum had 'inadvertently created a messaging service'. As Koum reflected, 'Being able to reach somebody halfway across the world instantly, on a device that is always with you, is powerful' (Olson, 2014a). Unlike Blackberry's BBM (Blackberry Messenger) which only worked on Blackberry phones and iMessenger which only worked on iPhones, WhatsApp worked across platforms, it was interoperable. Moreover, access to WhatsApp only required a phone number.

WhatsApp was designed against the ethos and method of Silicon Valley startups popular at the time, as Acton explained to Wired UK: 'We're the most atypical Silicon Valley company you'll come across. We were founded by thirty somethings; we focused on business sustainability and revenue rather than getting big fast; we've been incognito almost all the time; we're mobile first; and we're global first' (Flore, 2015). The value of WhatsApp was its simplicity: prioritizing user experience over ad generation. This was what attracted Jim Goetz of Sequoia Capital, a prominent venture capitalist in Silicon Valley, to the app: 'WhatsApp is simple, secure, and fast. It does not ask you to spend time building up a new graph of your relationships; instead, it taps the one that's already there. Jan and Brian's decisions are fuelled by a desire to let people communicate with no interference' (Flore, 2015).

When we began research for this project WhatsApp was a topic for niche technology publications or but a footnote in studies on (then) Facebook (McNamee, 2019; Levy, 2020; Frenkel and Kang, 2021). But WhatsApp was becoming *the* story in India, Brazil, Mexico Kenya, Indonesia and Nigeria where the simple messaging app was not only gaining in popularity as a place to connect with friends and family but the private nature of digital messaging spaces were increasingly enmeshed in transforming sociopolitical life. Between 2017 and 2018 reports emerged about an apparent correlation between WhatsApp, misinformation, violence and/or political corruption

in India, Brazil, Mexico, Sri Lanka and Indonesia (Wired, 2018). The bad press threatened to damage WhatsApp's reputation in key growth markets. Keen to deflect the attention and share responsibility, WhatsApp boosted relatively tiny research capacity by making 20 research awards to researchers worldwide. We were recipients of one of those awards for our proposal to research the social media and everyday life during the 2019 Indian elections (on the politics of Big Tech funding, see Williams et al, 2022). That research kindled ideas for this book, leading to more independent funding and further research. As WhatsApp's fortunes have shifted, our interest in the app has gravitated towards the (geo)politics of private messaging spaces and the stories that WhatsApp tells us(ers), governments and itself about privacy to advance its corporate power and profit. In 2021, ProPublica reported that a 49-slide internal company marketing presentation they acquired emphasized the 'fierce' promotion of WhatsApp's 'privacy narrative' (Elkind, Gillum and Silverman, 2021). WhatsApp's strategy to 'lean into' privacy has publicly, and privately, informed its transformation from a simple messaging app that generated little revenue into the 'the backbone of Meta's business' (Issac, 2023). Our critical privacy approach complements early books on WhatsApp that chart the evolution of WhatsApp into a 'global communication and business platform' (Johns, Matamoros-Fernández and Baulch, 2023), studies the everyday life of WhatsApp through extreme speech (Udupa and Wasserman, 2025), surveys how WhatsApp is embedded within Indian society (Narayan and Narayanan, 2024) and examines WhatsApp's role beyond misinformation in West Africa (Hassan and Hitchen, 2022). At a time when WhatsApp is now (finally) popular in the US market there is a risk that we might forget or fail to realize how an ordinary app that is now so embedded within our socio-economic and political lives came to be that way.

WhatsApp's petri dish? The global south, India and building a public utility

Although located in Silicon Valley WhatsApp's initial growth markets were outside the US with the largest of these in the global south, notably India, Brazil, Malaysia, Indonesia, Mexico, Kenya and South Africa. There were two sides to the product's geography. On the one hand, WhatsApp was originally less appealing to the domestic US market. In the US, mobile messaging was very competitive with flat pricing for SMS and free minutes whereas data bundles were more expensive. Moreover, internet-based messaging services such as Facebook messenger and iMessage on iPhones were established messaging platforms. This made the case for adopting WhatsApp far less compelling in the US than in areas where SMS attracted itemized billing or where Facebook and the iPhone were less ubiquitous.

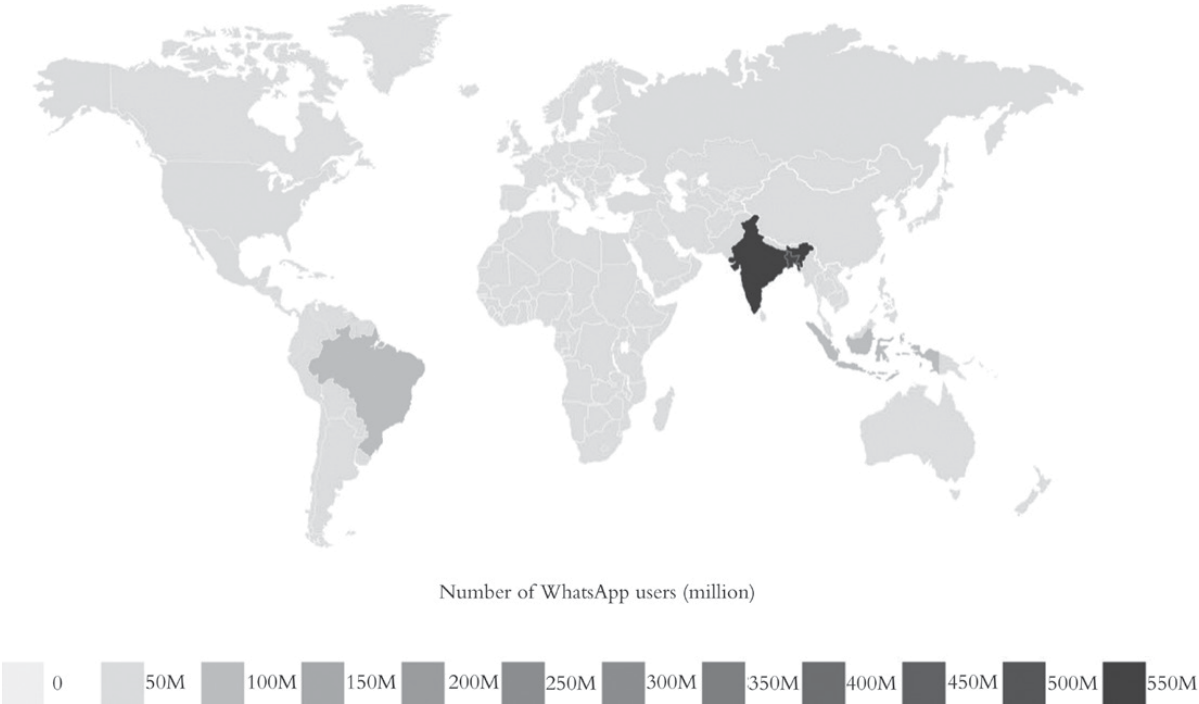
Domestic users in the US were typically those with friends and family abroad and/or those who travelled, for instance Hispanic and South Asian populations.

On the other hand, WhatsApp was more attractive to international markets. In the global south, the simplicity and low-data usage of WhatsApp found traction in economies where access to the internet prevailed on smartphones with relatively affordable data packages. By ‘leapfrogging’ laptop and desktop computer use with smartphones, people’s initial access to the internet was often through WhatsApp. Using WhatsApp on smartphones overcame the limits of poor broadband infrastructure as well as the expense of SMS and conventional voice calls. But it also enabled the integration of text with video, audio, emoji and other multimedia content which gave the messaging app broad appeal. Voice notes and emojis afforded those with limited literacy the means to communicate on the platform. Another dimension to WhatsApp’s simplicity concerned the fact that phone numbers rather than personal identifiers were considered the ‘user’. With phone contacts automatically pulled into WhatsApp on download, networks were therefore ready to build by messaging contacts and creating groups. WhatsApp made it possible to connect with groups as well as individuals and join emergent broadcast lists disseminating the latest news and updates thereby cultivating a sense of shared community (Baulch, Matamoros-Fernández and Johns, 2020).

Globally, India is easily WhatsApp’s largest market and it continues to grow, seeing growth of 16.6 per cent in 2023–2024 (see Figure 2.1). What happens with WhatsApp in India matters to Meta and its economic future. Though Meta does not officially share country wise user data, figures estimated from different sources suggest that since WhatsApp’s India launch in 2010, it has attracted over 500 million users (Kumar, 2025a). The rapid and continued growth of WhatsApp in India should be read in conjunction with a programme of state-led digitization extended by Prime Minister Narendra Modi in partnership with technocrats, Fintechs, software and telecoms companies (Nilekani and Shah, 2016; Dattani, 2019). A central pillar of ‘Digital India’ has been the development and operationalization of the National Optical Fibre Network to bridge India’s digital divide through the expansion of its internet and broadband infrastructure (Bhat, 2020). Between 2014 and 2024 the number of mobile broadband connections grew from 70 million to 906 million (Waghmare, 2024).

Using the internet on smartphones also became more accessible to more people with the availability of cheap Chinese smartphones in tandem with the dramatic reduction in the cost of data. In 2016 Reliance, India’s largest telecommunications company, launched Jio Life which provided some of the cheapest data packages in the world and effectively enabled free and reliable transmission of messages, graphics and voice calls as well as videos on platforms like WhatsApp. The introduction of WhatsApp video calling

Figure 2.1: Top 10 countries by WhatsApp users, 2024



Source: Naveen Kumar (2025) and Worldpopulationreview.com. Graphic: Cat Rawlins.

in 2016 was a catalysis for boosting downloads, while WhatsApp felt more intimate and less cluttered, rarely overwhelmed by the kind of junk messaging so prolific on SMS. By 2018 WhatsApp had 200 million monthly active users and the Wall Street Journal reported how Google researchers in Silicon Valley were left puzzled as to why one third of India's smartphones were freezing up daily. The answer was WhatsApp and a flourishing new morning ritual sending good morning messages to friends and family (Purnell, 2018; see also Venkatraman, 2017). Drawing on research in South India, Shiram Venkatraman (2017) argues that 'good morning' messages represent a digital expression of the Indian desire to build good karma. Sending everyday salutations and inspirational, often religious, messages not only maintained everyday group sociality, but became part of the daily routine of doing good to achieve favourable outcomes in the afterlife. However, the volume of good morning messages was also one of the reasons why young people chose to mute or leave family WhatsApp groups.

The family WhatsApp group was a place for reinforcing kinship through digital sociality and the proliferation of such groups across national and transnational contexts underpins why WhatsApp has so powerfully captured the Indian imagination (Gajjala and Verma, 2018). The 'WhatsApp University' has become a popular idiom for the source of all false information, meanwhile the 'WhatsApp Uncle' is an archetypal influential figure, parodied for being susceptible to misinformation and sensationalism, having a prolific message forwarding habit, strong opinions and pseudo-scientific propaganda which worsened during the COVID-19 pandemic (Khatri, 2024). WhatsApp had captivated a population of digital citizens unlike in any other market and Meta determined that India would be WhatsApp's 'petri dish for experimenting' (Cornish, 2023).

To say that India is *WhatsApp's* 'petri dish' belies a more vibrant, complex reality in which WhatsApp is also a place for *Indian* experimentation. This book is importantly about how India's user-citizens have domesticated WhatsApp's digital private spaces in novel, unanticipated and entrepreneurial ways. Global changes to WhatsApp's code and campaigns have often been prompted by what is happening on its app in India. Today WhatsApp is not only a place to connect and share with friends and family or local community and work groups but also where you sign up for the latest sports news or party-political updates (see Chapter 4). WhatsApp is how you buy groceries, receive prescriptions from the doctor, access cinema tickets and obtain updates on your Amazon order, find out your bank balance and get paid or watch the latest film trailer. It is not just businesses that partner with WhatsApp but also the Government of India. As part of the state's drive to build its digital public infrastructure, citizens can contact the government's helpdesk chatbot on WhatsApp and are advised to use WhatsApp to access their official documents like PAN (primary account number) cards, driving

licenses and insurance documents from DigiLocker, a cloud document storage wallet developed and implemented by the Ministry of Electronics and Information Technology. In the south Indian state of Andhra Pradesh, this partnership is now called ‘WhatsApp governance’ (Rao, 2025).

In India, WhatsApp has become a public utility through a combination of accident and design, built on top of a private digital messaging service. And, as a public utility WhatsApp is now a significant private authority; a Silicon Valley-based corporation delivering a digital public service in India. This book explores how the discursive and technical development and defence of WhatsApp’s privacy architectures have been key to building private corporate power in India and beyond.

Privacy architectures and privacy power

Ari Waldman has argued that corporate privacy agendas are not what they may seem, they are often complex and contradictory. WhatsApp is a lens for examining how private power has been advanced through privacy architectures that appear to serve its users while normalizing ever-expansive data extraction practices for profit. Corporate privacy practices can be anti-privacy in reality (Waldman, 2021). By privacy architectures we mean the discursive, technical, legal and affective dimensions of WhatsApp. That is, WhatsApp’s affordances, privacy policy, end-to-end encryption code, media messaging and interviews, legal documents and more. But we also refer to how WhatsApp operates – as a product of Meta, it is a private company that wields degrees of private authority acquired through its privatization of digital space.

Prior to Facebook’s acquisition, the original vision for WhatsApp was expressed through values of simplicity, reliability and security. The app’s interface and architecture were simple, they would not sell or place advertisements on WhatsApp. Acton and Koum’s aversion to advertisements was twofold: ads polluted users’ encounters with digital products and detracted from authentic personal engagements, after all, ‘No one wakes up excited to see more advertising, no one goes to sleep thinking about the ads they’ll see tomorrow’ (WhatsApp, 2012b). Their conviction was reinforced in their response to a competitor’s attempt to malign their intentions: ‘So first of all, let’s set the record straight. We have not, we do not and we will not **ever** sell your personal information to anyone. Period. End of story. Hopefully this clears things up’ (WhatsApp, 2012a, emphasis in the original).

Acton and Koum’s approach to data collection was minimalist. Writing on their blog they emphasized that when a company relies on advertisements for revenue, users’ data is what matters most to them. This means that ‘a significant portion of their engineering team spends their day tuning data mining, writing better code to collect all your personal data, upgrading the

servers that hold all the data and making sure it's all being logged and collated and sliced and packaged and shipped out. ... Remember, when advertising is involved **you the user** are the product' (WhatsApp, 2012b, emphasis in the original). Whereas Acton and Koum insisted that, at WhatsApp, the user's 'data isn't even in the picture. We are simply not interested in any of it' (WhatsApp, 2012b, emphasis in the original). Their goal was to deliver the 'best possible user experience' (WhatsApp, 2019).

The second underlying principle was that WhatsApp should be a 'secure' messaging platform that governments could not interfere with. This was informed by Koum's experience growing up in a village near Kiev, Ukraine. He recalled that under the surveillance state of the USSR his 'parents rarely talked on the phone in case it was tapped by the state' before escaping the country's political volatility and anti-Semitic environment with his mother and settling in the US in 2016 (Olson, 2014b; WhatsApp, 2014b). In the early days of WhatsApp, the emphasis was therefore on not using ads, not collecting user data other than the minimum and maintaining a secure app. Although the notion of privacy was implicit in WhatsApp's original vision, the term 'privacy' was not explicitly used by Koum and Acton in their early interviews or blogs about the product, preferring instead to talk in terms of safety and security. We show how WhatsApp's privacy architectures – its material, legal and discursive relationship to privacy – have been strategically developed following WhatsApp's purchase by Facebook in 2014. That WhatsApp with its commitment to minimal data collection and security would be transformed by Facebook's data capitalism machinery is not surprising, *how* Meta has patently promoted privacy and private spaces in the pursuit of data and profit *is* striking and needs surfacing.

The integration of Facebook and WhatsApp's technical infrastructure necessitated updating the company's legal position concerning its approach to data sharing with Facebook. Although undermining WhatsApp's original commitment to data minimalism, the new privacy policy was accompanied by public 'privacy talk' intended to deflect users' and regulator's concerns. Coding end-to-end encryption by default marked another shift in WhatsApp's privacy architecture with privacy-by-design now fully embedded in the app by 2016. End-to-end encryption offers the best in industry security for WhatsApp users, but it also produces the privatization or enclosure of digital private spaces by a private corporation.

In India, WhatsApp's subterranean digital private networks have enabled political parties and the powerful to prosper, evading accountability while augmenting WhatsApp's network power (see Chapter 4). End-to-end encryption also affords WhatsApp a form of code power which can be transformed into corporate power with respect to both user-citizens to cultivate trust as protectors of their privacy and to resist government requests for data. But the boundaries of data privacy have also been subject to legal

scrutiny and activism following WhatsApp's 2016 and 2021 privacy policy updates. Indeed, the ongoing struggle (at the time of writing) between the Indian government and WhatsApp/Meta is over questions of authority, data and privacy norms (see [Chapter 5](#)). The concept of privacy architectures captures the multiplicity of the material, technical, discursive and affective power of privacy with respect to WhatsApp.

With its dominance in the Indian market, WhatsApp's presence crystallizes debates about the relationship between privacy, people and power in interesting ways, and in particular questions about what privacy means to different people, who it's for, how it's designed and legislated and ultimately how privacy is actually experienced by ordinary people. More importantly, focusing on privacy through the case of WhatsApp in India shifts the lens away from western experiences and institutions: privacy, places, people and politics vary across geographies. How a Silicon Valley startup like WhatsApp is designed and imagined, delivered and domesticated looks very different depending on where you are, and who you are ([Chapters 6 and 7](#)). What this means for WhatsApp, for India and for democracy is what this book is most interested in. The next section contextualizes the growth of WhatsApp and how it 'landed' in India.

WhatsApp techtonics: 'one billion plus people'

Connecting: Facebook, WhatsApp and the 'rest of the world'

Zuckerberg posted news of WhatsApp's acquisition in a typically upbeat post: 'Jan and the WhatsApp team have done some amazing work to connect almost half a billion people. I can't wait for them to join Facebook and help us connect the rest of the world' ([Zuckerberg, 2014](#)). Zuckerberg had finally closed the deal on WhatsApp, two years after his first approach. For Zuckerberg, 'it is better to buy than compete' ([Neate, 2020](#)).

Having carefully protected the values and vision of WhatsApp not only from Google but also TenCent's advances, Acton and Koum were finally cajoled by Zuckerberg who 'came with a large sum of money and made us an offer we couldn't refuse' (Acton cited in [Olson, 2018](#)). By February 2014, WhatsApp had more than 450 million daily active users and more than one million new people signing up every day ([Facebook, 2014a](#)). Not only was WhatsApp challenging the dominance of Facebook messenger, but WhatsApp was growing in markets that Facebook was yet to access in the global south. Zuckerberg's fear was that if people adopted a data light messaging app like WhatsApp to connect with family and friends, they would be less inclined to sign up to Facebook ([Vox Media Podcast Network, 2022](#)). In 2012, Zuckerberg had concluded that WhatsApp was 'legitimately a better product for mobile messaging than even our standalone Messenger app' and '[u]nfortunately for us, I don't think there's any way to directly

minimise the advantage which is their momentum and growth rate’ (Neate, 2020). Zuckerberg needed WhatsApp at any cost to safeguard his company’s monopoly on connecting the world and there too, the global ‘attention economy’ (Wu, 2016).

The deal was rapidly finalized over a February weekend in 2014. WhatsApp was acquired for \$19 billion, the largest internet deal to date. The European Commission reported the purchase details: ‘Facebook is making the purchase in a mix of cash and stock. WhatsApp will receive \$12bn in Facebook shares \$4bn in cash and an additional \$3bn in restricted shares that will be paid out to executives at a later date. The company will operate as an autonomous unit’ (European Commission, 2014b). Preoccupied with closing the deal, Zuckerberg was reportedly agreeable to Acton and Koum’s ban on ads as well as their emergent designs to encrypt WhatsApp which would prohibit any ambitions to extract data from users’ messages (Olson, 2018).

The narrated appeal of WhatsApp to users in the global south – light on data, accessible on smartphones, secure messaging – and apparent organic uptake of the app, belies a more complex picture of the situated regulatory, technical, economic, social and political contexts in which WhatsApp ‘landed’ and became domesticated. In particular, it risks downplaying Facebook’s explicit role in extending the reach of WhatsApp to parts of the global south where Facebook was so far less widespread and hoping to attract users through its ‘non-profit’ initiative. As Zuckerberg projected in a quarterly earnings call in 2014: ‘Over the next few years, we’re going to work hard to help WhatsApp grow and connect the whole world. We also expect that WhatsApp will add to our efforts for Internet.org, our partnership to make basic internet services affordable for everyone’ (Zuckerberg 2014). WhatsApp would therefore bolster the ambitions of internet.org for individuals in the global south as an ‘on ramp’ to the internet. It was clear that by helping Facebook to ‘connect the rest of the world’, Zuckerberg saw in WhatsApp the potential to reach the next billion users and these users were in the global south.

Facebook’s primary objective for WhatsApp was the growth of its MAUs. This was underpinned by a strategy which focused on ‘connecting 1 billion plus people’ and *then* monetizing the private messaging app. As Zuckerberg argued ‘once we get to that scale, then we think that they will start to become meaningful businesses in their own right’ (Facebook, 2014b). It was very important to Zuckerberg not to rush to monetize WhatsApp (or Instagram or Facebook messenger) but to let them reach their ‘full potential before very aggressively turning them into businesses’ (Facebook, 2014b).

Facebook and Mark Zuckerberg’s preoccupation with growth has been widely documented in popular and cultural productions. Ben Grosser’s creative intervention surfaces Zuckerberg’s fetish with growth. Grosser’s epic supercut splices film of the Big Tech CEO’s utterances of ‘more’,

‘grow’ and/or metrics like 1 billion or 2 billion from his public appearances between 2004–2019. Called ‘Order of Magnitude’, the 50-minute-long film animates and amplifies the underlying logic of a company that is determined to monopolize our digital connections and attention (Grosser interview with the authors 2023).

The singular focus on driving user growth and scaling up was reinforced in Facebook’s Q3 2015 Earnings Call when Facebook’s Chief Financial Officer responded to a question by an equity research analyst concerning how and when Facebook planned to monetize WhatsApp:

The focus really for our messaging products is to continue to drive user growth and continue to build great products that are fast, useful, engaging and fun ... the business side is not the main focus right now but we believe there are going to be opportunities as we further scale those properties. (Facebook, 2015)

Protecting and growing WhatsApp’s user base depended on there being or indeed creating the infrastructure to support that growth as well as safeguarding against potential competition from elsewhere. Facebook had already been exploring ways to gatekeep internet access.

Gatekeeping: going mobile, zero rating and the failure of Free Basics

Access to the internet in the global south is almost universally on mobile. The practice of zero rating – providing internet access using ‘free’ data or ‘minutes’ on a phone contract – is another important part of the geographical story concerning the growth of WhatsApp. It tracks back to the launch of Facebook Zero which was a lighter version of the core app that ‘suppressed data intensive features such as photos and videos’ – the intention being that the app could be made available for free and help Facebook ‘make the social network as ubiquitous on mobile phones as possible’ (TechCrunch, 2014). Facebook established a relationship with some telecommunication companies (mobile or internet service providers) that enabled them to provide users access to some services and applications with no cost to their data allowance.

The Facebook Whistleblower, Francis Haughen, was particularly critical of the implications of zero rating. In Brazil, for example, mobile app packages usually include Meta’s platforms such as WhatsApp, Facebook and Instagram with Waze, Twitter and TikTok sometimes also added (Spagnuolo and Martins, 2022). This in part explains the huge dependence on WhatsApp in Brazil, even when Brazilians run out of data they can still access WhatsApp on their phone, moreover, for many, WhatsApp or ‘ZapZap’ as it is known locally, is the internet (Barbosa, 2023). In an interview with Núcleo, Haughen surmised that Facebook’s motivation for zero rating was a fear of

competition or anti-competition agenda in their emerging markets, ‘they were afraid TikTok was going to emerge ... they were afraid Brazil was going to invent the next form of social media’. Zero-ratings worked for both telecom companies and Facebook by accelerating the adoption of the mobile web (Spagnuolo and Martins, 2022). But, the rapid rise of WhatsApp was met with opposition from Brazil’s Telecoms companies who responded by lobbying to limit WhatsApp’s growth in the country; they claimed WhatsApp was unregulated and illegal and publicly blamed the ‘WhatsApp effect’ for driving millions of Brazilians to abandon their cell phone lines (see Pereira, Bueno Bojczuk Camargo and Parks, 2021).

Unlike in Brazil, zero rating was prohibited in India when efforts by Facebook to introduce internet.org were thwarted by public and government opposition. Internet.org is a Facebook-led not-for-profit venture committed to connecting the poor and disconnected and providing not only a ‘free’ internet service but also vital digital literacy skills. Free Basics was the alternative name given to internet.org as Facebook continued, despite critiques, to reach new markets by providing basic internet services in areas with poor internet infrastructure on mobile phones but without depleting users’ data plans (Wynn-Williams, 2025). Facebook delivers this service in collaboration with mobile operators and zero-rated offerings on a few sites, including Facebook and specific partners for weather and news such as Accuweather, Ask.com, Bing search, Wattpad, WikiHow and Wikipedia.

But Indian internet activists, led by the Internet Coalition, pushed back on these plans. They were opposed to a few content providers creating a ‘walled garden effect’ around their internet services. This granted them unfair access to first-time internet users who had few incentives to explore alternatives. Furthermore, Facebook (and other companies) could mine users’ data thereby compromising privacy and security. As Nishant Shah explained: ‘What internet.org was saying was that because they are doing you a favour, because they are giving this away to you for free, they get to decide what you get to access and you cannot hold them accountable for it’ (Shah, 2016).

Subhayan Mukerjee’s research documents how the Free Basics approach was counterintuitive to the principles of ‘net neutrality’ where the power to decide who had access to what data or content could be determined by new internet gatekeepers. For Tim Berners-Lee, ‘it’s not internet. It isn’t free, and it isn’t in the public domain. Giving people data connectivity to only a part of the network deliberately, I think is a step backwards’ (cited in Mukerjee, 2016, p 358). Zuckerberg did not agree and spent \$45 million aggressively promoting Free Basics with billboards, newspaper advertisements and an op-ed in the *Times of India* intended to persuade the public to ‘choose facts over fiction’. In this Zuckerberg railed against critics of Free Basics who he claimed were unfairly denying free digital access and essential services to India’s ‘disconnected’ (Zuckerberg, 2015a). In 2016 the Telecom Regulatory

Authority of India (TRAI) ruled against a subset of the internet being made available, it did not mention Free Basics directly but instead argued that zero-rated internet schemes infringed upon the principles of net neutrality (Vincent, 2016).

This emergent internet activism and ultimate ruling by the TRAI proved to be a seminal moment in India, both for Facebook and Indian citizens for whom fair and equal access to the internet was constructed as a human right (Zuckerberg, 2015a). Siva Vaidhyanathan points out that ‘Facebook officials not only underestimated the opposition within India, they had failed to pay attention to the particulars of the Indian political economy’ (Vaidhyanathan, 2018, p 113). Moreover, as Nishant Shah argues it was also the first-time concerns were raised about the ‘neo-colonialist’ attitudes of a Californian company who understood little about the needs and lives of underprivileged Indian citizens. With the internet tantamount to a human right, the ‘rights of citizens’ were potentially being bypassed by a private American company drawing up contracts based on its ‘terms of service’ (Shah, 2016). Indian citizens had spoken, Facebook could not and would not be a gatekeeper to their internet.

Siva Vaidhyanathan has expertly demonstrated how Facebook’s ‘relationships with states, users, and other commercial services are dynamic’ and the company has a tendency for ‘morphing and metastasising’ (2018, p 115). Against the backdrop of Free Basics’ failure in India, Facebook shifted its full attention to the potential of WhatsApp whose fortunes were being fortified by the ‘Digital India’ programme. Indians now had access to some of the cheapest data packages in the world which effectively enabled free and reliable sharing of messages, graphics and voice calls as well as videos on platforms like WhatsApp. Through WhatsApp, Facebook would succeed in parcelling up the internet into private digital spaces for sharing information. For people accessing the internet for the first time on mobile, WhatsApp *was* the internet, and it had their attention.

Sharing: the WhatsApp attention economy

Growing WhatsApp entailed not simply connecting people but increasing the volume and velocity of ‘sharing’ on the platform: the sharing of voice calls and notes, texts, videos and memes as well as one’s location. As Zuckerberg explained on the third quarterly earnings call in 2014

Our mission is to make the world more open and connected. We do this by building services that help people share any type of content with any group of people they want. WhatsApp will help us do this by continuing to develop a service that people around the world love to use every day. (Zuckerberg, 2014)

Unlike other social network sites the practice of ‘sharing’ has remained a constitutive activity of WhatsApp (John, 2012, 2024). For example, the front page of WhatsApp’s website explained to users that: ‘Some of your most personal moments are shared on WhatsApp, which is why we built E2EE into the latest versions of our app’ and consistently invited us to ‘Share your location’.

In contrast to SMS text messaging, WhatsApp facilitated the creation and organization of private group chats, administered by individuals who determine the group’s membership of up to 256 members when adding manually. While group chats are ostensibly ‘private’, people with a link can also gain ‘public’ access to groups, thereby increasing the size of the group chat. Crucially, as WhatsApp gained popularity, group chats engendered the potential for information to ‘go viral’ through practices of sharing and ‘forwarding’ digital content within networks of private digital spaces.

The exchange of digital objects, GPS coordinates and our thoughts contrasts with the ‘likes’, ‘posts’ and ‘clicks’ more characteristic of the data generated and abstracted in the ‘attention economy’ (Davenport and Beck, 2001; Terranova, 2012; Wu, 2016b). Defined by theoretical physicist Goldhaber, the ‘attention economy’ is a ‘system that revolves primarily around paying, receiving and seeking what is most intrinsically limited and not replaceable by anything else, namely the attention of other human being’ (Goldhaber cited in Chamorro-Premuzic, 2014). Social networking sites that deliver ‘zero cost products’ must compete for users’ attention which can be transformed into ‘a kind of capital’. Terranova has argued that the ‘abstract quality of attention’ in combination with ‘the fact that the “attentional assemblages” of digital media enable automated forms of measurement (as in “clicks”, “downloads”, “likes”, “views”, “followers”, and “sharings” of digital objects) open it up to marketization and financialization’. The result, ‘[a] whole new data processing and mining industry ... born on the back of social qualities harvested which literally reflect the social distribution and intensity of attention’ (Terranova, 2012, p 66).

WhatsApp acquires its value through the intensity of its networked user engagement and ability to continually capture *and* maintain users’ attention over time. Tim Wu explains in ‘Attention Merchants’, that conceived of as a resource, attention is understood as both scarce, limited by the 168 hours that we each have in a week and as something that cannot be stored or hold value over time, as such it must be continually accessed (Wu, 2016). The ability to share information reliably with minimal friction and at scale is a key part of WhatsApp’s success, after all WhatsApp measures its growth not just in terms of MAUs, but also the number and type of messages sent on its platform and users’ attention to those messages.

Back in 2013, when interviewed on stage at the industry conference ‘D: Dive Into Mobile’, Jan Koum announced that WhatsApp had acquired

more users than Twitter, which officially claimed 200 million monthly active users at that point. He was also keen to broadcast that WhatsApp was processing 8 billion inbound messages and 12 billion outbound and moreover, that the vast majority of people who used WhatsApp used it every day ('active daily users') (Gannes, 2013). And again, on publicizing the news that WhatsApp had reached 'half a billion people around the world' who were 'regular, active WhatsApp users' the emphasis was on the fact that 'users are also sharing more than 700 million photos and 100 million videos every single day' (WhatsApp, 2014a). Koum was also eager to emphasize that users valued the uncluttered interface with WhatsApp and reiterated his opinion that when brokering attention for advertising: '[t]he user experience would always lose, because you always had to provide a service to the advertiser'. Moreover, because '[c]ellphones are so personal and private to you ... putting an advertisement there is not a good experience' (Gannes, 2013).

WhatsApp had succeeded in capturing users' attention by crossing 'into what were purely private or social spaces' (Wu, 2016, p 23), building networks of those private digital spaces and not flooding the app with intrusive adverts. When interviewed a few weeks after Facebook had acquired WhatsApp, Zuckerberg defended the high purchase price despite WhatsApp's low revenue on the grounds that WhatsApp was the 'most engaging' messaging app:

Already almost half a billion people love using WhatsApp for messaging and it's the most engaging app that we've ever seen exist on mobile by far. About 70 per cent of the people who use WhatsApp use it every day which kind of blows away everything else that's out there. (YouTube, 2014b)

The challenge now facing Facebook was how to monetize WhatsApp's 'attention economy' without undermining the consumer experience on WhatsApp itself and losing their attention.

Monetizing WhatsApp: eroding privacy, making 'a meaningful business'

News of Facebook's purchase of WhatsApp in 2014 had been met with concern and caution from both the US's Federal Trade Commission (FTC) and the EU Commission who stressed the companies' contradictory approaches to data relations and warned against the degradation of WhatsApp's service with its stated commitment to minimal data collection and message security. In response to regulatory and media commentary Koum and Acton sought to reassure users about the future of WhatsApp as part of Facebook.

If partnering with Facebook meant that we had to change our values, we wouldn't have done it. Instead, we are forming a partnership that would allow us to continue operating independently and autonomously. Our fundamental values and beliefs will not change. Our principles will not change. Everything that has made WhatsApp the leader in personal messaging will still be in place. Speculation to the contrary isn't just baseless and unfounded, it's irresponsible. It has the effect of scaring people into thinking we're suddenly collecting all kinds of new data. That's just not true, and it's important to us that you know that.

Make no mistake: our future partnership with Facebook will not compromise the vision that brought us to this point. Our focus remains on delivering the promise of WhatsApp far and wide, so that people around the world have the freedom to speak their mind without fear. (WhatsApp, 2014b)

Despite the public messaging and reassurance that WhatsApp would not change after the merger, soon after WhatsApp was purchased it dropped the nominal annual subscription fee and Facebook's senior management debated plans to monetize WhatsApp (Levy, 2020, p 502). Two options were under consideration. The first concerned publishing targeted ads in WhatsApp's Status feature and the second looked at building tools for businesses to chat with their customers. Acton wasn't opposed to monetizing WhatsApp *per se*, but he was opposed to the concepts on the table. Talking to Olson (2018), Acton recalled his alternative proposals, such as inviting businesses: 'to send "informational, useful content" to WhatsApp users, like the SMS from his Honda dealer, but don't allow them to advertise or track data beyond a phone number' or his proposal to monetize WhatsApp by 'charging users a small amount once they exceeded a large number of free messages'. As Acton explained, Sheryl Sandberg, then Facebook's Chief Operating Officer, did not take to his plan, suggesting that 'it won't scale'. But reading between the lines, Acton understood that what Sandberg really meant was that it 'won't make as much money'; there were other more data rich avenues to pursue.

Monetizing WhatsApp would require the expansion of data collection and data sharing. In mid-2016 Mark Zuckerberg made the case that Facebook should have access to WhatsApp's data and integrate some of WhatsApp's and Facebook's services. Acton and Koum reluctantly agreed to the move and took pains to negotiate the nature of changes to WhatsApp's 2012 terms of service that such a move would entail. Acton and Koum opposed Facebook's request for 'broader rights' to WhatsApp user data. They came away with a compromise which retained their ban on ads, but Facebook and WhatsApp accounts would be linked so users could be targeted with friend suggestions and Facebook's advertising partners could improve their targeted ads on Facebook.

Such changes represented a fundamental shift in WhatsApp's privacy and data relations with Facebook and with users and were quietly actioned through the company's 2016 Privacy Policy, an update to the 2012 Privacy Notice. As the Electronic Frontier Foundation reported 'WhatsApp is establishing data-sharing practices that signal a significant shift in its attitude toward privacy – though you wouldn't know it from the privacy policy update that popped up on users' screens last week' (Gebhart, 2016). The benign and confusing language of the update meant its implications largely evaded the scrutiny of ordinary users, however European regulators and activists notably in India, raised concerns about the legality of the updates and their implication for users' right to privacy. This major rupture in WhatsApp's privacy principles was trailed by a public statement from WhatsApp seeking to redirect the more critical voices and assert the company's commitment to privacy, that was genomically embodied in the app:

Respect for your privacy is coded into our DNA, and we built WhatsApp around the goal of knowing as little about you as possible: You don't have to give us your name and we don't ask for your email address. We don't know your birthday. We don't know your home address. We don't know where you work. We don't know your likes, what you search for on the internet or collect your GPS location. None of that data has ever been collected and stored by WhatsApp, and we really have no plans to change that. (WhatsApp, 2014b)

This moment marked a public, material shift in how WhatsApp (and Facebook) actively promoted its privacy vision to build trust with users, while simultaneously un-making privacy relations to enhance Facebook's access to users' metadata behind the scenes.

Another development at this time was the implementation of end-to-end encryption by default on WhatsApp. This security code had the potential to complicate Zuckerberg's ambitions to monetize WhatsApp. Encryption was available on the app from 2012, but end-to-end encryption promised far greater security for personal communications by ensuring that third parties – such as an internet service provider, application service provider, hacker or any other entity – cannot 'read' the data while it is being transferred. The data is encrypted and decrypted by cryptographic keys located on the devices or systems of the sender and intended recipient only. While initially blasé about the implications of end-to-end encryption Zuckerberg later questioned the plans 'in terms of business value' (Levy, 2020, p 501). Zuckerberg's concern was that without the capacity for Facebook to read the messages and convert the information into data that could inform better user experience, new services or more efficient targeted ads, Facebook would be 'leaving money on the table' (Levy, 2020, p 501). But as we show in Chapters 5 and 6, although

end-to-encryption curtailed Facebook's access to personal information, it carried code power that WhatsApp productively mobilizes when negotiating with national governments or when appealing to ordinary users about their commitment to data privacy and security.

By 2017, the ruptures over privacy and data opened a rift between Zuckerberg and WhatsApp's co-founders. Acton was uncomfortable with the groundwork being laid for targeted ads and commercial messaging and quit Facebook later that year. He left behind \$850 million in stock still owed from WhatsApp's sale rather than sign a non-disclosure agreement proposed as part of a settlement deal (Olson, 2018). Koum soon followed in 2018. The departure of WhatsApp's co-founders coupled with the continued growth of users opened the way for Facebook to intensify plans to transform WhatsApp 'into a meaningful business in its own right' (Facebook, 2014b). Since the fallout of the Cambridge Analytica scandal, Facebook had spent the last couple of years focused on 'the major social issues facing the internet and our company' and making 'heavy investments' 'in safety, security privacy and, well-being' rather than building new products (Facebook, 2018a).

By the end of 2018 Zuckerberg announced that 'I ... feel like we have started to turn a corner and have a clear plan for what we need to do here now. Moreover, "Messaging" was "the area that's growing the most quickly" with the expectation that this year [2019] people are going to feel these [messaging] apps becoming the center of their social experience in more ways' (Facebook, 2018a). The evolution of WhatsApp into a tool for business communication would be key to that shift. Beta testing for WhatsApp Business and WhatsApp Pay was rolled out in India and Brazil from 2018. In India, Reliance JioPlatforms partnered with Facebook both on the launch of JioPhone 2, a feature phone pre-installed with YouTube, Facebook and WhatsApp and on JioMart a new ecommerce venture with the 'ordering system' on WhatsApp in 2020. Meanwhile Facebook was acquiring startups such as Kustomer (Tech, 2018; Singh, 2020). This dynamism led the *New York Times* to observe that 'WhatsApp is being remodelled in front of our eyes. Watch what happens because even if you don't use the messaging app, the changes could reshape the direction of the internet' (Ovide, 2020).

But before WhatsApp for Business could be fully realized in India, further amendments to WhatsApp's privacy policy were required that recognized how the platform's data including messages would be shared with businesses and other third parties. From January 2021 all WhatsApp users were required to 'Agree' to the new terms of service or lose access to the app entirely. The policy clarified what information was already being shared with Facebook companies, for example a user's phone number, transaction data, interaction data, device information and IP address. And it also announced changes to how commercial companies that users interact with on WhatsApp or the 'third party service providers' with whom those businesses work, can 'access

... communications to send, store, read, manage, or otherwise process them for the business'. In other words, business could use customers' conversations as well as their metadata to perform data analytics, train machine learning models, or use it for targeted advertising.

By 2021, there was a new public understanding of Facebook's untrustworthy data relations which meant that unlike in 2016, WhatsApp's update *was* met with a public 'backlash' as media headlines proclaimed: 'WhatsApp battles privacy concerns in India – its biggest market' (Jazeera, 2021), 'WhatsApp Delays Privacy Changes Amid User Backlash' (Vega, 2021), 'WhatsApp uses millions of users after terms update' (Hern, 2021) and 'Govt again warns WhatsApp to scrap the 2021 privacy policy' (Aryan, 2021). We argue that how WhatsApp (and Meta) responded to users' concerns as well as the media, government and legal challenges to its plans to commercialize attention on the platform is an exercise in WhatsApp's (and Meta's) private authority and platform sovereignty. The struggle over privacy ideas and practices is a privacy game and a necessary aspect of techno-feudalism.

The power of WhatsApp's private authority is made manifest in today's digital-political economy, for while legal challenges against the 2021 privacy policy continue in the Indian courts, and elsewhere, WhatsApp is now very much *in* business. Facebook doesn't break down the income of its family of products (Instagram, Facebook messenger, WhatsApp and Threads), but estimates suggest that in 2018 WhatsApp's annual revenue was \$443 million compared with \$1.3 billion in 2023 with WhatsApp Business generating most of WhatsApp's revenue (Gratton, 2024). As of February 2024, India dominated the global share of WhatsApp Business with 481.2 million downloads compared to the second largest market, Indonesia which had 128.4 million downloads (Bhagchandani, 2024).

Weaponizing encryption

Meta's journey to monetizing WhatsApp must be read alongside the technical boundaries and discursive possibilities afforded by end-to-end encryption. As noted by WhatsApp, end-to-end encryption keeps personal information beyond the surveillance and reach of 'cybercriminals, hackers, and rogue states' (WhatsApp, 2016a). In our digital lives, encrypted messaging infrastructures are an undeniably useful and vital utility for ordinary citizens. And yet, the subterranean nature of WhatsApp, the fact that information shared on its networked private spaces and publicly accessed groups is beyond the realm of public scrutiny and accountability means that WhatsApp can and is being 'weaponised' by the 'bad actors' and 'rogue states' whom WhatsApp claims to protect its users from (WhatsApp, 2016a). The fine balance between the importance of information security for users' communications to both be and 'feel' private and the challenges facing governments and Big Tech in

preventing, detecting and prosecuting malpractices within encrypted spaces is currently widely debated (also see Apple, Telegram). This has implications for democracy, individual privacy and national security as Sabeena's earlier account illustrated.

Taking 'privacy' as the subject, we are concerned with how WhatsApp's encrypted digital messaging spaces have been weaponized and promoted, often for purposes that are fundamentally anti-democratic and antithetical to WhatsApp's original vision. Of particular interest is how the debates arising from these challenges variously attract different actors – WhatsApp, government, civil society, citizens – presenting contrasting conceptions of privacy and security, responsibility and accountability. As is so often the case with technology, there are inevitably the unintended, unanticipated outcomes and vulnerabilities within a technical system. For WhatsApp, this has entailed the weaponization of digital private spaces for the mass circulation of mis/disinformation, hate speech and the propagation of automated computer propaganda more often for political purposes, but also scam or junk messaging as well as the exploitation of WhatsApp by state sponsored spyware. The prevalence and impact of these practices has been most acutely felt and reported on in WhatsApp's early and largest markets, notably India and Brazil (Chakrabarti, Stengel and Solanki, 2018; Banaji and Bhat, 2019; Cesarino, 2019; Evangelista, 2019).

As early as 2016, reports emerged in India about incidents of violence, locally referred to as 'lynchings' which were connected to rumours shared on social media including on WhatsApp and which functioned to incite violence. These rumours often evoked the threat of strangers stealing children, harvesting organs or slaughtering cows and informed the killing or violence against individuals (Arun, 2019). IndiaSpend recorded that between January 2017 and July 2018, 33 people had been killed in 69 incidents of mob violence (Saldanha, Rajput and Hazare, 2018). By July 2018 such stories were making national and international headlines with a correlation drawn between the violence, 'fake news' and the rise of WhatsApp in India. The Government of India confronted WhatsApp highlighting 'the large number of irresponsible and explosive messages filled with rumours and provocation ... being circulated on WhatsApp' and the killing of people in Assam, Maharashtra, Karnataka, Tripura and west Bengal (PIB, 2018b). What followed were a series of exchanges between the Government of India and WhatsApp, with the Ministry of Electronics and IT placing the blame on WhatsApp's technology and calling for the company to 'take immediate action to end this menace and ensure that their platform is not used for such malafide activities' (PIB, 2018b).

The government were insistent that WhatsApp 'cannot evade accountability and responsibility specially [sic] when good technological inventions are abused by some miscreants who resort to provocative messages which lead to spread of violence'. Responding in a letter to the ministry, WhatsApp

shared their horror at recent violent events but challenged the claim that their origin and, therefore also, solution, lay in WhatsApp's technology alone. 'We believe that false news, misinformation and the spread of hoaxes are issues best tackled collectively: by government, civil society and technology companies working together' (Phartiyal, 2018).

WhatsApp perceived their responsibility to lie in better educating WhatsApp users about the risks of 'fake news' on the one hand and on the other, making subtle adjustments to WhatsApp's architecture to influence how people interact with the technology. In the first instance WhatsApp moved to label forwarded messages as 'forwards' to help users 'determine if your friend or relative wrote the message they sent or if it originally came from someone else' (WhatsApp, 2018a). And therefore to provide a pause 'to encourage you to think' before sharing messages that were forwarded (WhatsApp, 2018a). This update was soon followed by 'a test to limit forwarding' that would be applied globally but 'In India – where people forward more messages, photos, and videos than any other country in the world – we'll also test a lower limit of 5 chats at once and we'll remove the quick forward button next to media messages' (WhatsApp, 2018b). Despite these edits to WhatsApp's code, the further death of a software engineer in Bidar, Karnataka in connection with the viral circulation of child kidnapping rumours on WhatsApp provoked a further response from the Government of India. This time they called for 'bringing in traceability and accountability when a provocative / inflammatory message is detected, and a request is made by law enforcement agencies'. The Government of India held the 'medium' of information – WhatsApp – accountable and argued that 'If they remain mute spectators they are liable to be treated as abettors and thereafter face consequent legal action' (PIB, 2018a).

The disputes over misinformation and encryption threatened to overshadow if not delay WhatsApp's ambitions to test its business products in India. Chris Daniels, then CEO of WhatsApp, travelled to New Delhi in October to meet with government ministers and business leaders. Speaking to the Economic Times, Daniels evoked WhatsApp's privacy principles and the materiality of its encryption infrastructure to push back on the government's request to trace the original sender of a message, as he explained: 'To do this, we would have to redesign our systems and revise our privacy standards to indiscriminately track user data. We think this is overly intrusive from a privacy perspective.' The primary focus for Chris Daniels' visit was to explore how WhatsApp 'could support Indian businesses and drive economic growth'. He appealed to India as 'the world's largest democracy' and 'as a nation that values competition, economic empowerment for all, privacy, and respect for individual rights'.

As WhatsApp continues to grow in popularity in India, it's my hope that we can continue to provide great products that improve

the lives of the people of India and make doing business easier. It's thrilling to see that there are over one million users of WhatsApp Business products in India. ... With our full set of features in place for both people and businesses, we believe WhatsApp will continue to contribute to economic growth here in India. (Singh, 2018a, 2018b; see Chapter 8)

The relationship between WhatsApp and the Government of India led by the Bharatiya Janata Party (BJP), who remain in power at the time of writing, is complicated. Not only does the government of India use WhatsApp for its internal organizations and the delivery of government services and accountability, but the BJP was quick to recognize the potential of WhatsApp for winning elections. Widely understood as a right-wing Hindu nationalist party, the BJP has an established and well-resourced 'IT cell' that has consistently capitalized on social media for political capital, from Twitter to Facebook and more recently WhatsApp (Schroeder, 2018). Shivam Shankar Singh – ex volunteer for the BJP tuned campaigner – documents the close relationship between data analysts, some of whom, like Singh, had returned from jobs as software engineers in Silicon Valley to collaborate with party-political workers and exploit data analytics for political power (Singh, 2019). WhatsApp was one tool used by this newly emerging class of political consultants working in the 'backstage of democracy' (Sharma, 2024).

WhatsApp's private digital spaces provided the potential for disseminating targeted campaign messages, a strategy that was initially refined in India's state elections and then rolled out more widely during the 2019 national elections and again in 2024. The BJP's 'playbook' resembles that of classic populist right politics prevalent in Trump's United States or Orban's Hungary. The BJP and its proxies use WhatsApp to produce and amplify divisive imaginaries through subterranean storytelling which augments affective nationalist and populist energies. The repertoire of digital content reflects mundane marketing of the government's achievements and promotion of Narendra Modi as a cult personality as well as decontextualized videos, manipulated images and more recently 'deep fakes' typically aimed at undermining India's minority communities' and particularly its Muslim citizens' humanity (Sinha, 2017; Banaji and Bhat, 2019; Tech, 2019). The emotive nature of content intentionally exploits people's desire to share and 'forward' messages out of 'civic duty' as well as political interests such that messages travel at volume and speed from large and obviously political groups, channels and communities through private networked groups of family, community and friends as part of a larger digital ecosystem (Chakrabarti, Stengel and Solanki, 2018; Banaji and Bhat, 2019). Encounters between WhatsApp and the Government

of India and particularly in their struggles over the ‘right to privacy’ and security need to be read within this context as we begin to further explore in [Chapter 5](#). But first we provide an account of privacy techtonics and the conceptual and empirical research that informs the book’s arguments concerning a feminist geopolitics of privacy.

Privacy Techtonics

Privacy Techtonics is a feminist geopolitics framework for critically examining privacy in the context of Big Tech, state, society and data relations. It is a speculative framework that opens up our understanding of the shifting intimate and global relationships between digital technologies, data and privacy in a multiplicity of ways. As a speculative framework, *Privacy Techtonics* is intended to integrate a scalar, relational and material approach to thinking about digital privacy. It playfully draws on the analogies of ‘tectonics’ and a ‘tonic’ to inform our enquiry and gestures to Big Tech and feminist technoscience’s proclivity to metaphorical ways of knowing the world (Haraway, 1985).

Tectonics riffs on the term ‘tectonics’ meaning ‘of or relating to building or construction’ (etymoline), derived from the Late Latin term ‘*tectonicus*’ and which stems from the Greek ‘*tektonikos*’ ‘pertaining to building’ and ‘*tekton*’ meaning carpenter, builder, master in any art’. ‘Tec’ has its roots in the proto- Indo-European root ‘*teks*’ meaning ‘to fabricate’ or ‘to weave’ which also relates to the Sanskrit ‘*taksati*’ meaning ‘he fashions, constructs’. The term tectonics underpins the geological study of ‘plate tectonics’ relating to the large-scale processes and material properties of the earth’s crust (for a racial critique, see Yusoff, 2024). The process of ‘plate tectonics’ helps to explain the surface or topography of the earth’s landscapes caused by shifts in the tectonic plates and interpreted through the sensing of the subterranean processes beneath the earth’s crust. These dynamics are more often invisible on the surface though periodically find expression on the surface of the earth. They are sensed on or near plate boundaries and fault lines, produced by ruptures, friction and erosion of the earth’s crust which produce tremors, reverberations and transformations in the landscape over space and time.

The analogy to global plate tectonics productively locates the relationship between privacy and digital technologies within a planetary scale. Ben Bratton (2015) proposes the speculative imaginary of ‘planetary scale computation’ to capture the reality of the internet as more than social media and the smartphone. This ‘computational totality’ is the outcome

of an ‘accidental megastructure’ of hardware and software technologies comprising a multiplicity of things, layers and actors that it assembles and is assembled through and which acts like a ‘planetary-skin’ enveloping the earth. As we show, discursive and material shifts in digital privacy and the private are shaped by intersecting planetary forces and pressure of technology, governance and social norms. These shape and are shaped by regulations or designed frictions around data sharing, such as privacy laws and policies, the code that determines user behaviour, boundary-making practices, discourses and the transformation of privacy norms. An important dimension of our approach to digital privacy is to sense the shifting relationships between privacy, power and (geo)politics, examine the discursive and material struggles that are implicated in privacy fault lines and boundaries and examine the relational connections that produce (new) privacy topographies.

Following feminist technoscience and feminist geopolitics, situating knowledge production and experience is central to our enquiry into digital privacy and the private within a planetary context which we do by prioritizing a relational understanding of the ‘things, layers and actors’ that shape privacy techtonics in place (Haraway, 1988, p 54; Wajcman, 2004). Here, the adoption of tectonics within architectural practice and critique is also instructive for conceiving of ‘a language of architecture’ that reveals how diverse architectural elements – design, materials, regulations, culture/subjectivity, and systems – are integrated into coherent meaningful entities that are also built and engender an embodied and affective experience, *somewhere* (Frampton, 2001). As Frew writes: ‘Tectonics ... infuses [structures] with a sense of place, purpose and identity by bridging design, materials, construction methods and structural logic’ that are experienced (Frew, nd).

Scholars have conceptualized digital platforms as ‘digital architectures’ that are ‘an empirically observable object of analysis’ and encompass ‘the technical protocols that enable, constrain, and shape user behavior in a virtual space’. The digital architecture underpins a platform or app’s affordances (Bossetta, 2018, p 473). In thinking about digital private messaging we are interested in how ‘a platform’s specific design features affect particular communication practices’ (Bossetta, 2018, p 474), and find that conceptualizing digital architecture importantly also makes visible the broader ‘political and economic forces that seek to order societies and dominate our human future’ (Flyverbom, 2022, pp 6–7). For instance, ‘[a] social media’s digital architecture is written in code, influenced by algorithms, and constantly edited by developers to maintain a competitive market advantage’ (Bossetta, 2018, p 473). For WhatsApp we conceive of privacy architectures as integral to its digital architectures which ‘captures more than technical features so as to encompass the complexity and richness of technological, social and commercial forces that propel and shape them’ (Flyverbom, 2022, p 5). Like architecture tectonics, *Privacy Techtonics* seeks to reveal the process by which

WhatsApp's privacy architecture is designed, constructed and assembled and is constitutive of both material as well as cultural, political and ethical life (Frampton, 2001).

Finally, following Zuckerberg's speculative private future we suggest that 'tonic' also be read as a playful metaphor for something that refreshes, restores or stimulates. Privacy as tonic is intended to capture the concrete and performative work that 'privacy' and the 'private' does for Facebook and WhatsApp's fortunes. As metaphor it also mimics a preferred linguistic technique used by Silicon Valley to communicate and embed their technology products in our everyday lives. We discuss this in more detail later in the chapter. But first we start by locating privacy, privatization and private authority within recent global transformations. Next, we situate privacy and the case for the decolonization of privacy studies before illustrating the complex relationship between privacy and power. In the fourth section we introduce scholarship that surfaces the political dimensions of privacy. Section five contextualizes privacy, data and democracy within India's post-colonial context followed by the case for 'sensing' privacy through the 'domestication' of both privacy and geopolitics and attending to its material and affective dimensions. In the penultimate section we return to the idea of privacy as a 'tonic' and conclude by outlining the book's research methods.

Tectonic shifts: private authority, privatization and digital private spaces

Our enquiry into the feminist geopolitics of digital privacy is situated at the intersection of three key shifts that concern: the global rise of Big Tech and its private authority; the privatization of the internet and our data lives and; finally the shift from digital public spaces to more private interactions. In the last 30 years Meta, Google, Twitter and Amazon, Baidu, Alibaba Tencent and Xiaomi have become techno-oligarchs, all through the trade of mainly personal data and the emergence of the data economy. This hugely successful business model has been exported to other institutions – to the 'surveillance society' (Lyon, 2001) and 'surveillance capitalism' (Zuboff, 2019), 'data capitalism' (West, 2019) and 'informational capitalism' (Cohen, 2019a) – and which inform the emergence of a 'planetary scale computation' that is reconfiguring nation state geopolitics (Bratton, 2015).

The largest technology corporations are wealthier and more powerful than many nation states. Big Tech leaders (or 'bros') flanked the stage at the recent inauguration of President Donald Trump while Meta's CEO, Mark Zuckerberg figuratively and literally embraced India's Prime Minister, Narendra Modi in 2015 soon after he was first elected to power. Swati Srivastava locates Big Tech's global scale and influence in its 'algorithmic governance', in other words, its capacity to organize the world's information

and connections and thereby shape social ordering through the automation of machine decision making which is trained on the vast amounts of data they collect (Srivastava, 2021). Algorithmic governance mediates the relationship between Big Tech corporations and nation states, where Big Tech cooperates by sharing data at the request of law enforcement but on the other hand Big Tech also has a history of pushing back against government. For example, Apple have recently withdrawn ‘advanced data protection’ from customer’s iCloud storage rather than acquiesce to the UK government’s demand to create a ‘backdoor’ so that it can access users’ data. Apple had earlier refused the FBI’s plea to share the information contained on the iPhone of the San Bernadino shooter (Gill, 2018; Kleinman, 2025). Srivastava captures this complex dynamic when she writes: ‘Algorithms mediate the scope of these oscillating matchups as states become dependent on Big Tech, Big Tech circumvents state overreach, and states curtail Big Tech’ (Srivastava, 2021, p 990).

That Big Tech can resist or refuse to engage with government’s requests at all speaks to the private authority that Big Tech increasingly wields, underpinned by its private governance of digital infrastructures that deliver public utilities (Balkin, 2017). As Balkin argues,

[p]rivate governance means that the infrastructure provider governs the flow of information through the infrastructure that it owns, and it governs the behavior of the end-users and customers who employ the digital infrastructure. The ability to govern comes from telecommunications law, from infrastructure owners’ property rights, and from their contractual agreements with end-users. (Balkin, 2017, p 36)

Technology companies such as Facebook whose ‘predecessor site’ was designed ‘to help horny Harvard students rate the hotness of people in nearby dormitories’ now finds itself operating with the scope and power of a nation state (Lewis, 2021). As Zuckerberg observed in an interview with the Guardian: ‘In a lot of ways Facebook is more like a government than a traditional company ... We have this large community of people, and more than other technology companies we’re really setting policies’ (Foer, 2017). Though as Sarah Wynn-Williams reveals in her recent memoir on working as a Vice President at Facebook, Mark Zuckerberg took some persuading that he and Facebook had to take global policy and politics seriously (Wynn-Williams, 2025).

Through digital infrastructures and algorithmic governance, techno-oligarchs ‘claim to be, perform as, and are recognized as legitimate by some larger public (that often includes states themselves) as authors of policies, of practices, of rules, and of norms’ (Hall and Biersteker, 2002, p 4). Within

an evolving technology and regulatory space, technology corporations establish their private authority through ‘entrepreneurial’ practices ‘in which private actors create rules or set standards without the explicit delegation of authority by states’ (Green, 2014, p 78) and then promote these ideas as norms to those who comprise the governed. Sympathetic to this argument, Julie Cohen makes visible how Big Tech actors ‘mobilize legal tools and institutions to advance their goals’ (2019b, p 241). Whereas Zuboff’s (2019) thesis claims that ‘surveillance capitalism’ functions because of its lawlessness, Cohen (2019b) insists that ‘informational capitalism’ is a function not of the absence of law, but of intentional struggles over legality and its operations at the ‘edge of the law’ (Jeffrey, 2019). Big Tech’s private authority is reinscribed at the boundaries of legal and social norms and policies. As we explore in Chapter 5 determining the meaning and legal boundaries of privacy is an important location of struggle between Big Tech, the state and society.

When governments move to moderate big tech’s private authority through regulation, they come under pressure from its significant lobby network. Between 2020 and 2022 Meta spent \$19–20 million a year on lobbying, making it one of the top spenders on lobbying in the US, more than the arms and aircraft manufactures, Lockheed Martin and Boeing. Speaking on the Joe Rogan podcast soon after the re-election of President Donald Trump, Mark Zuckerberg used the opportunity to criticize the European Union for having ‘fined the tech companies more than 30 billion’ in recent decades and urged the new US government to play a role in ‘basically defending [‘the US tech industry’] abroad’ (The Joe Rogan Experience, 2025). The private authority of technology corporations means that they can reshape the policy process and seek to establish themselves as key actors in that process, thereby enabling a ‘self-perpetuating cycle of escalating benefits for Big Tech’ (Khanal, Zhang and Taeihagh, 2024). ‘What differentiates authority from power is the legitimacy of claims of authority’ (Hall and Biersteker, 2002, p 4). But a technology corporation’s legitimacy with a ‘larger public’ can be vulnerable to public challenge or erosion by competitors’ actions; maintaining legitimacy therefore requires ongoing work with the public – its users, for authority to be positively recognized. A feminist geopolitical approach to global power and authority reorientates our attention concerning dominant forms of knowledge away from nation state actors and the pursuit of hard power to build a broader framework that is open to plural and relational sites and practices of power (Enloe, 1989; Dowler and Sharp, 2001; Hyndman, 2004, 2019).

The second related shift concerns how technology corporations have extended their power and authority by progressively privatizing the internet through the dual production of digital enclosures and the privatization of private life. Although originally conceived of as the internet commons built on Open Access protocols, technology companies have progressively

parcelled up the internet into private ‘digital enclosures’ – ‘the creation of an interactive realm wherein every action, interaction, and transaction generates information about itself ... in which every virtual “move” has the potential to leave a digital trace or record of itself’ (Andrejevic, 2009, p 53). Building on critical accounts of capitalism the process of enclosure is understood as the means by which information that was actually or potentially in the public domain becomes private property (see also Boyle, 2003) and so, ‘entry into the digital enclosure carries with it, in most cases, the condition of surveillance or monitoring’. The comparison to England’s land enclosure movement is illustrative of ‘the transformation of violent expropriation into freely agreed-upon contractual arrangement’. Though in this case, there are those who control new privatized interactive spaces and newly created private resources and ‘those who submit to forms of monitoring in order to gain access to goods, services, and conveniences’ (Andrejevic, 2009, pp 54, 55).

As Varoufakis observes, ‘In the eighteenth century, it was land that the many were denied access to. In the twenty-first century, it is access to our own identity’ ... ‘our digital identity belongs neither to us nor to the state. Strewn across countless privately owned digital realms, it has many owners, none of whom is us’ (Varoufakis, 2024, p 72; see also Cohen, 2019a; Durand, 2024). In the data economy, ‘digital fiefdoms’ therefore derive their power from amassing and processing personal data; value is extracted to predict behaviour or influence individuals or groups and drive corporate profit (Zuboff, 2019; Véliz, 2021; Varoufakis, 2024).

‘Big data’ and ‘the digital’ more generally are seen as constituting new frontiers to be ‘explored, expanded and conquered’ (Thatcher, O’Sullivan and Mahmoudi, 2016, p 993). Analogized to a process of ‘data colonialism’,

[p]reviously private times and places are commodified and privatised as a new terrain for capital investment and exchange. Further these processes occur in the context of an asymmetrical power relation between individuals whose actions generate individual datums and those who come to own and profit from the big data they become. Finally, the asymmetrical extraction of value is shown to presume both quantification and surveillance of the lifeworld, of lived experience, as a natural, desired experience of modern life. (Thatcher, O’Sullivan and Mahmoudi, 2016, pp 991–992)

Developing this metaphor further, Couldry and Mejias argue that ‘data colonialism’ is the appropriation of ‘human life through its conversion to data’ which is an extension of ‘a global process of extraction that started under colonialism and continued through industrial capitalism’ (Couldry and Mejias, 2019, p xix).

The third intersecting shift which underpins *Privacy Tectonics* is the pivot from digital public to digital private messaging spaces. We are particularly interested in the impact of WhatsApp's private or subterranean digital networks for political and democratic life in India and relations between Big Tech, the state and citizens. [Chapter 1](#) introduced the context within which Meta projects the digital private space and private communications as the future, at once a strategic move to sustain its ongoing global expansion especially within the global south.

Reflecting on events between 2010 and 2015 which included the Arab Spring, scholars have documented how public digital platforms such as Twitter and Facebook have transformed the quality of democratic practices; evoking new forms of expression, affiliation and 'affective publics' as well as enabling the rise of computer-aided elections ([Gerbaudo, 2012](#); [Papacharissi, 2014](#); [Gonzalez, 2017](#)). Earlier too, in a challenge to European normative theories that democratic life is realized within the public sphere ([Habermas, 2005](#)), new digital private networks of citizens were understood to represent active sites of political life and citizenship ([Papacharissi, 2010](#)). Conceptualizing democracy as the distribution of power between private and public spheres, Papacharissi argues that digital technologies have transformed how connections are formed between individuals and how power is distributed, with the digital private sphere offering new possibilities for civic connections and dissent. She contends that '[t]o the extent that the private sphere affords the autonomy, control, and expressive capabilities that enable dissent, it effectively reconciles the personal with the political in a way that enables connection with like-minded individuals' ([Papacharissi, 2010](#), p 167). And moreover, the 'meaning of the political lies in the ability to express dissent, to think differently' ([Papacharissi, 2010](#), p 166).

That liberal euphoria around the internet's potential to democratize knowledge and power has given way to a more dystopian reality characterized by right-wing and populist exclusionary discourse, what Udupa, Gagliardone and Hervik, call a new 'global conjuncture of digitally enabled exclusionary politics' ([Udupa, Gagliardone and Hervik, 2021](#), p 12). In India, WhatsApp's end-to-end encrypted messaging has proven to be a potent platform for the Hindu right to circulate 'extreme speech' ([Udupa and Pohjonen, 2019](#)), hate speech ([Banaji and Bhat, 2022](#)) and misinformation that finds traction and circulation among an electorate motivated by civic duty and a commitment to nation building ([Chakrabarti, Stengel and Solanki, 2018](#)). As Tom Boellstorff writes, '[v]irtual worlds do not mediate between places; they are places in their own right that persist as individuals log into and out of them' ([Boellstorff, 2016](#), p 394). And as others have documented, digital and physical spaces are intertwined through everyday life ([Willems, 2019](#)).

In the context of shifting public-private boundaries and digital-political life, *Privacy Tectonics* shows how digital private places in India have become

encoded with neo-Hindutva logics and the boundaries between digital-physical experiences blurred in the (re)production of a Hindu nationalist future (Anderson and Longkumer, 2018). As such, it is important to recognize how digital private places are increasingly central in political experience and geographies of democracy more broadly. We understand democracy as the balance between private and public, digital and physical spaces, which prompts us to question how democracy finds local expression through registers of sociality, relatedness, difference and agency (Paley, 2002). As Barnett and Low (2004, p 15) argue,

the virtue of democracy inheres in the quality of relations between different imperatives, interests, and identities – that is, it lies in the degree of openness to contestation of definitions of the proper balance between imperatives of collective action and individual freedom, between conflicting interests, and between multiple and fluid identities.

Privacy Tectonics seeks to understand how these intersecting and multiscalar shifts in privacy and the private interact with and are constitutive of political and democratic life in India. Before we introduce the wider debates concerning privacy and democracy in India, we present the intellectual arguments for why a feminist geopolitics of digital privacy is so important.

Situating privacy

Privacy Tectonics responds to a timely imperative to decolonize privacy studies through an everyday and situated approach to understanding the contours of Big Tech's private authority, digital privacy and the private in India. Such an approach acknowledges the continuities between colonialism and capitalism in Big Tech and makes visible 'the colonial core of today's data practices' (Couldry and Mejias, 2023, p 794). Framing the case for the 'decolonisation of privacy studies', Payal Arora calls for the ongoing need 'to recognize the deeply structured, essentializing and historically reproduced power asymmetries within social and technical norms, knowledge, values, and infrastructures' (2019a, p 367).

Digital privacy in the 'digital peripheries' concerns the lives of racialized and gendered people in the north and south for whom experiences of privacy and data are disproportionately read through the lens of security and surveillance. For racialized and gendered subjects of surveillance, privacy is peripheral: it is inferred as a lack or a luxury; denied to individuals who are not worthy of it, and knowingly or unknowingly traded by those who cannot afford it (McGlotten, 2016; Eubanks, 2018; Benjamin, 2019). Alice Marwick argues that compared to surveillance studies, privacy studies has been relatively slow to embrace critical racial and feminist approaches to

studying privacy in ways that centre and critically engage with ‘questions of marginality, inequality, power, and empire’ (Marwick, 2022, p 397). Marwick reasons that while there are exceptions, privacy studies typically draws on legal, experimental or computer science approaches which often lack ‘a deep analytic of global, state, corporate, or interpersonal power differentials’ (Marwick, 2022, p 397).

Consequently, privacy studies tends to prioritize individual privacy behaviours, privacy harms, privacy violations and mitigation through regulation and technical design. Yet, this approach ‘implicitly frames privacy as an end state to be achieved or protected, without examining how the nature of privacy itself is constituted, or may be transformed, through these practices’ (Elwood and Leszczynski, 2011, p 7). By integrating a critical approach to privacy that centres a feminist relational ontology of power *Privacy Tectonics* recognizes that all practices are situated and implicated in the politics of everyday life (Marston, Jones III and Woodward, 2005) and are context dependent (Nissenbaum, 2009). Adopting a relational approach prioritizes situated, contingent and fragmented experiences, norms and practices of privacy in the everyday, and how they are entangled and connected across topographies (Katz, 2001).

Privacy Tectonics questions existing geographies of privacy studies, which as Arora argues are ethnocentric and continue to disproportionately draw on ‘empirical evidence on privacy attitudes and behaviours of Western-based, white, and middle-class demographics to theorize privacy in this digitally mediated world’ (Arora, 2019a, p 368). It is also the case that for privacy studies, privacy perceptions, harms, values, experiences and norms of individuals and communities in the global south have been perceived to hold less relevance and therefore visibility when it comes to understanding, designing and forming legal and regulatory practices or sociotechnical systems (Arora, 2019a, p 368). A potential explanation for this partial perspective lies in the colonial legacies of disciplinary knowledge production and power where the global south is read through the narrow lens of ‘development’ (Arora, 2019b). Where development and big data projects are engaged ‘there is a bias in framing big data as an instrument of empowerment in the global south’ (Arora, 2016, p 1682). And relatedly for ‘governments, technology companies, and elite multilateral organizations’ to work in partnership to use populations in the global south publics ‘as testbeds for innovations in technological surveillance’. This leads Arora to conclude that ‘privacy concerns thereby would be marginal to this agenda’ (Arora, 2019a, p 368).

The call to decolonize privacy studies dialogues with scholarship on ‘computing in/from the south’ (Milan and Treré, 2019; Amrute and Murillo, 2020; Mertia, 2020; Masiero, 2022). This movement explicitly challenges tendencies towards ‘data universalism’ (Milan and Treré, 2019, p 1) which narrate the ‘data revolution’ from an exclusively western perspective and erase

the diverse experiences of people and data in most of the world (Masiero, 2022). Recognizing this tension between capturing a global shift towards data colonialism *and* the particular situated nature of its impacts (see also Couldry and Mejias, 2023), Arora urges that '[d]ecolonial scholars should not shy away from the particularities of globalization of privacy values, norms, and practices while dismantling pervasive universalisms in the process' (Arora, 2019a, p 375).

Privacy Techtonics responds by challenging privacy frames that privilege 'Western concerns, contexts, and user behaviours' (Arora, 2016, p 1682) and examining the interaction between universalizing and normalizing privacy narratives and the situated practices through which privacy finds expression such as privacy stories, legal artifacts and proceedings, technical design and lived experience. It engages with digital feminist geographers' call for new insights into the 'digital mediations of complex bodies, lives, places, politics, economies and socialities in ways that challenge longstanding disciplinary exclusions' (Elwood and Leszczynski, 2018, p 630). By doing so we also offer a rejoinder to Arora (2019a) by showing how in the case of WhatsApp, privacy is *central* not marginal to the company's political and economic profile in India and beyond. As WhatsApp's largest market by far, India is also *central* not peripheral to the making of WhatsApp. India is a crucial 'test bed' or laboratory for WhatsApp to innovate and develop its product for dissemination globally. But this is not a one-way process, India also *makes* WhatsApp. For as Véliz reminds us '[t]echnology doesn't happen to us – we make it happen' (Véliz, 2021, p 73). Similarly, WhatsApp doesn't happen to India – India makes it happen.

Privacy and power

At the heart of *Privacy Techtonics* is a critical approach to the relationship between privacy and power. In recent years, critical scholars of informational privacy have surfaced the power dynamics that inform Big Tech's data and privacy narratives, shape legal and regulatory frameworks and become embedded within social relations as everyday privacy norms. We examine the intersections of these arguments through the lens of privacy and data stories, asymmetrical power relations, performative privacy and re-working privacy.

Privacy and data stories

A decolonial approach to privacy situates privacy and 'today's data practices and uses of technology in terms of the historical *longue durée* of the past 500 years, not just the past 15 years of social media, or even the past 40 years of internet development' (Couldry and Mejias, 2023, p 796). An important dimension of this concerns the claims that Big Tech makes to justify and

legitimize their expanding data extraction processes within the global south which are anchored within ‘larger frameworks of rationality, progress, order, science and modernity (even salvation!)’ (Couldry and Mejias, 2023, p 796). Privacy stories and their narratives are therefore influential in shaping how we understand what privacy is, who it’s for and why it matters. Those in power shape these narratives and when it comes to informational privacy, Big Tech leaders currently dominate our privacy imaginaries by promoting and manipulating what appears obvious and common sense concerning the nature and value of data and the means to realize data privacy.

The expansion of the ‘social quantification sector’ through the exploitation and extraction of social resources or personal data concerns the normalization or naturalization of ‘data relations’ (Couldry and Mejias, 2019). As privacy law scholar Neil Richards writes: ‘Technology companies have described their processes of data collection as somewhere between a natural, benign activity and the recycling of an unclaimed resource—the “data exhaust”—that would otherwise go to waste’ (Richards, 2022, p 42). Drawing on feminist and critical geopolitics makes us attentive to how discourses can actively obscure the ‘coloniality of power’ (Ricaurte, 2019), and how this depends on and reproduces an uneven politics of privacy that makes data relations possible in the first place. Data relations are sustained through innumerable data privacy violations, manipulations and encroachments which are also made to look normal or benign. A key concern for us is how privacy is simultaneously asserted by Big Tech as a public good while also serving to conceal its private commercial interests.

In other scenarios companies will insist that the personal data that is shared is important for innovating and personalizing their services which are an inevitable aspect of technological progress and primarily for users’ benefit (Véliz, 2021, p 71). The computer scientist, Jaap-Henk Hoepman (2021) calls these ‘privacy myths’ because they conceal from users the ‘real’ value of their (meta) data to Big Tech, downplay the relevance of privacy in particular settings or relationships and tacitly persuade users to continue sharing their data which enables Big Tech to continue collecting personal, and other data, for profit. By intervening in data centric narratives, Hoepman (2021) foregrounds the actual practices and relationships that exist behind the data, between Big Tech platforms, executives, software engineers, regulatory actors and users, among others, and who come to constitute privacy processes.

On the other hand, discourses that assert the universal positive values of privacy also serve to reflect the narrow interests of those in power by drawing on an abstracted and ahistorical account of privacy and applying it as a universal human principle that applies to the experience of all individuals and societies everywhere. Social media scholar Christian Fuchs argues that universalizing narratives ‘tend not to engage with actual and possible negative effects of privacy or the relationship of modern privacy to private

property, capital accumulation, and social inequality’ (Fuchs, 2017, p 192). Writing from a critical Marxist perspective, Fuchs calls out the ‘liberal fetishism of privacy’ where liberal privacy theories ‘typically talk about the positive qualities that privacy entails ... without discussing the particular role of privacy in capitalist society’ (Fuchs, 2017, p 190). Fetishizing privacy as a universal ‘ideological mechanism’ can help ‘to reproduce and deepen inequality’ (Fuchs, 2017, p 187) and therefore foreclose the opportunity for critique and the recognition that privacy is unevenly experienced within different geographies and contexts.

In proposing a decolonial approach to data law and governance, de Souza, Mukiri Smith and Taylor grapple with the continuities between colonialism and capitalism when they question ‘who determines what is universal ... how these universal ideas and concepts circulate, and how they become stable’ (de Souza, Mukiri Smith and Taylor, 2024, p 4). They spotlight the ‘commodification of privacy’ by companies like Apple and Google through the creation of ‘privacy-enhancing technology’ as an example of how privacy as a universal idea is ‘operationalised’ (Pahuja, 2011 cited in de Souza, Mukiri Smith and Taylor, 2024). The reasoning is that Google and Apple ‘offer a technical solution which neatly fits within their business models and obscures the business logics that underpin a surveillance economy’ (de Souza, Mukiri Smith and Taylor, 2024, p 4). This case speaks to how technology companies intentionally manage and market the self-fulfilling interaction between privacy narratives and privacy things, as we further examine next.

Big Tech’s privacy and data stories may be contradictory but whether downplaying or highlighting the importance of privacy within different contexts, they are always consistent with commercial interests. Fuchs gets to the crux of this ambiguous relationship between Big Tech and privacy when he writes that:

Privacy in capitalism can best be characterised as an antagonistic value that is, on the one side, upheld as a universal value for protecting privacy property, but is at the same time permanently undermined by corporate surveillance in the lives of people for profit purposes and by political surveillance for administrative purposes, defence and law enforcement. Capitalism protects privacy for the rich and companies, but at the same time legitimates privacy violations of consumers and citizens. It thereby undermines its own positing of privacy as a universal value. (Fuchs, 2017, p 188)

Asymmetrical power relations

Informational capitalism ‘creates and enhances undesirable power asymmetries’ (Véliz, 2021, p 43). Asymmetrical power relations not only

characterize the data and privacy relationships between tech corporations, states and users, but also within and between different geographies and societies informed by the compounding effects of colonialism, capitalism and patriarchy. Privacy philosopher Clarissa Véliz points out that ‘Big tech’s power comes from what they take in personal data, not what they charge’ (Véliz, 2021, p 63). Tech companies’ power is constituted, ‘on the one hand, by having exclusive control of our data, and on the other, by the ability to anticipate our everyday move, which in turn gives them the opportunities to influence our behaviour, and sell that influence to others – including governments’ (Véliz, 2021, p 63). Big Tech companies are private entities and, as such, have the power and authority to determine what data they collect under what conditions and when and where those parameters are adjusted.

This evokes questions about the landscape and efficacy of data and privacy regulation with respect to digital technology companies. Julie Cohen, an American legal scholar, documents how in the US ‘information processing industries – including platform firms, data brokers and others – have advanced a carefully crafted narrative organized around the themes of innovation and deregulation’ (Cohen, 2019a, p 90). Innovation is portrayed as an ‘inevitably beneficial process’ that risks being encumbered by excessive, indeed any, regulation (Cohen, 2019a, pp 90–91). In response, regulatory regimes such as the Federal Trade Commission in the US have recognized the argument for autonomous market-led innovation by advancing the notion of a ‘balance’. As Cohen argues, it is important to situate this rhetoric of technological innovation which ‘derives from and mobilizes a distinctively American ideology about the power and promise of technology’ and acknowledge how technology corporations have successfully leveraged the law for their commercial interests (Cohen, 2019a, pp 91, 92).

Reading Igo (2018) or Gajda’s (2022) histories of the ‘right to privacy’ in the US also reminds us of the political, economic and cultural contexts within which ideas of privacy have been shaped, and how privacy has historically served the interests of patriarchy and privilege. Often anchored in the right to be left alone and protected from unfavourable publicity. The relationship between Silicon Valley Big Tech and users/society is therefore informed by US legal models of privacy that rest on the idea of ‘the individual as the liberal political subject: autonomous, rationale, separate from their body, and nothing like an actual person’ (Marwick, 2023, p 28). In this formulation, data is constructed as ‘personal’ to imply that the individual is ‘the only concerned party when it comes to sharing it’ and privacy is both an individual ‘right’ and regarded as a form of property that individuals own and have responsibility for protecting (Véliz, 2021, pp 88–89; see also Lessig, 2002; Gehl, 2016; Cohen, 2019b).

Alice Marwick challenges this ‘outdated’ idea that privacy is an individual concern in the context of today’s ‘internet networks’ which ‘reveal

information by connecting nodes intended to be separate.’ (Marwick, 2023, p 61). She argues that ‘[n]etworked structural threats make it impossible for any one person to protect their own privacy’. Especially where ‘networks overlap, connect, and leak to other networks, whose members may have different norms and discursive resources to interpret information’. Recognizing this, Marwick conceptualizes the importance of ‘[n]etworked privacy’ which incorporates ‘the intrinsic social and networked nature’ of privacy and therefore accounts for the fact that the impact of privacy violations will differ depending on ‘one’s location within a network and social hierarchy of power’ (Marwick, 2023, pp 31, 30, 31). Marwick’s feminist critique echoes the ‘relational turn’ to data privacy within legal spheres which seeks to spotlight the people and the relationships within which data is used, and account for the power imbalances between different parties (Richards and Hartzog, 2020; Viljoen, 2021).

Performative privacy

Acknowledging the power imbalance between technology companies and users, regulatory frameworks and corporate strategies have been implemented to reduce the information costs to individuals and the information asymmetry between individuals and companies. Julie Cohen argues that the US regulators’ acceptance that ‘privacy and innovation are in tension’ led to a framework where user choice and consent appeared as a convenient solution to this ‘dilemma’ (Cohen, 2019a, p 91). The ‘notice and consent’ model was implemented to ‘fill the regulatory gap’ concerning the use of online tracking techniques and the privacy policy become the ‘*de facto* vehicle for ensuring compliance’ (Cohen, 2019a, p 56).

Privacy policies have been roundly critiqued for being all but performative in practice. Privacy scholars have argued that privacy policies are often too ambiguous and long for the average user to engage with and meaningfully issue their consent (Reidenberg et al, 2015). The volume of applications, services and websites for which privacy policies are published means that users are confronted with an overload of information. To systematically process this information carries a significant time cost to individuals wishing to make informed decisions while others are left disempowered and disinterested by the prospect of reading lengthy, technical and legalistic documents (McDonald and Cranor, 2008; Cranor, 2012; Auxier et al, 2019). Research by Turow, Michael and Draper concluded that a large percentage of Americans do not understand the most basic aspects of privacy notification with misunderstanding highest among younger people and those from lower socio-economic and educational backgrounds (Turow, Michael and Draper, 2018). Moreover, the privacy policy proposition means that to exercise ‘choice’, users must be willing to walk away from valuable services if they

don't wish to consent to its terms of use (Vaidhyanathan, 2012). Consent is not a real choice; it is part of a performance by technology companies to convey confidence that they take users' privacy interests seriously.

Through his exposition of how Google operates, Siva Vaidhyanathan highlights the company's deceptive and contradictory trade practices by drawing attention to its 'fast changing "privacy policies"' which 'matter less than design choices' where 'the design of the system rigs it in favour of the interests of the company and against the interests of users' (Vaidhyanathan, 2012, p 84). In practice, the company's complicated and opaque data collection structures mean that 'Google's privacy policy is ... pretty much a lack-of-privacy policy' which gives Google 'substantial power over the data'. And although the policies state that it 'will not share information with other companies without user consent' it does have the right to share data with government and enforcement when required to do so (Vaidhyanathan, 2012, pp 84–85).

Privacy policies have evolved to protect the legal and commercial interests of technology companies while transferring the responsibility for data privacy on to individual users through a model of privacy self-governance. Through his research within information corporations, socio-legal scholar Ari Waldman documents how this dynamic is made to look obvious or common sense through the 'normalising performances' of privacy discourse that 'centres around notions of choice, consent, and control: in other words, that privacy is about making our own choices about what to disclose, when, and to whom'. He argues that '[i]t is a vision of privacy so narrow that it allows companies, their employees, and their allies to honestly say they care about privacy and still do little to improve privacy protections for their customers' (Waldman, 2021, p 6).

Yet, as Ari Waldman goes on to argue, '[p]rivacy-as-control ... is less a discourse about privacy than it is a discourse about corporate power and immunity from law' (Waldman, 2021, p 57). Drawing on Julie Cohen, he highlights the 'performance of accountability' as another mode of privacy compliance strategy by which technology corporations are able 'to express a generic commitment to accountability without ... meaningful scrutiny of the underlying process' (Cohen, 2019b, p 250 cited in Waldman, 2021, p 93). High-profile privacy campaigns, content moderation and new privacy features serve to reassure but also crucially redirect or misdirect the attention of both regulators and users away from the data practices that are most valuable to a corporations' commercial interests.

With most of the research on privacy policies emanating from the global north and more often narrowly dedicated to examining privacy policy literacy, there is little wider understanding of the social and geopolitical life of privacy policies. In other words, how are privacy policies socialized within different jurisdictions and social political contexts? As socio-legal contracts

between technology companies and users, how do policies come alive in context, how are they mobilized and given meaning by user-citizens, the law, government and Big Tech and with what implications?

Re-working privacy

In practice, the experience and materiality of privacy concerns more than technology, ‘data protection’ and ‘rationally’ engaging with a company’s privacy mechanisms of control, choice and consent. Rather, lived experiences of navigating privacy are located within the social and within uneven geographies of online and offline power. Learning from feminist, (geo) political and post-colonial theories, ‘subaltern geopolitics’ generatively engages with subaltern imaginaries and experience, and a position that is ‘not completely other, resistant or alternative to dominant geopolitics’, but concerns an ambiguous position of marginality that is neither “inside” nor “outside” (Sharp, 2011, p 271). The subaltern here is one who occupies an ‘ambiguous position of marginality’ from which they engage with geopolitics (Sharp, 2011).

Seeing digital privacy through subaltern epistemologies encourages enquiries that go beyond binary readings and critiques of geopolitics to consider agency as more than political resistance. In this vein, Payal Arora has documented the contradictory and diverse everyday privacy practices of teens living in lower-income settlements in Brazil and India. Her study goes beyond the binary framing of the ‘privacy rich’ and ‘privacy poor’ to show how ‘poor’ teens consciously navigate digital privacy practices in their everyday lives, sometimes ‘playing with privacy’ surveillance systems to evade surveillance, or maximize their interests (Arora, 2019b). Contrary to readings of marginalized communities as inevitably ‘privacy poor’ and devoid of agency under surveillance regimes, Arora demonstrates how teens in lower-income settlements in Brazil and India refuse this theory in practice; they collect data for their own intelligence and use digital technologies ‘to understand, to enjoy, to value and to protect privacy’ (Arora, 2016, p 200).

Centring questions of agency and equity, Alice Marwick advocates for a feminist concept of ‘privacy work’ which acknowledges the everyday, often invisible, work that individuals (and collectives) engage in to achieve a ‘desired level of privacy’, (re)claim agency and maintain their boundaries in the context of uneven privacy power geometries. She argues that ‘privacy work is unevenly distributed and privacy violations have greater consequences for marginalised people’ (Marwick, 2023, pp 63, 67). Through Marwick’s research with differently marginalized youth in the US she documents the ‘hacks’ that young people learn within their networked lives, to determine who has access to what information, when and where. Many had little faith

in technology companies to protect their privacy, believing that Facebook or Instagram could ‘listen’ in on them and felt the burden of performing privacy work beyond the technology company’s privacy affordances. Moreover, while many adjusted their privacy settings, social contexts influenced their decision making, for example when ‘blocking’ a particular individual for greater privacy might result in other undesired social consequences (Marwick, 2023, pp 71–74).

The agency involved in navigating and articulating privacy practices is also reflected in Nippert-Eng’s (2010) ethnography of privacy in a Chicago neighbourhood which makes visible the ‘boundary work’ as well as the fragility and ambivalence of realizing privacy in practice. Even while privacy is making a recent resurgence within academic and popular scholarship discussing ‘the fight for privacy’ and calling us to ‘take back control of your data’ (Véliz, 2021; Citron, 2022), the philosophical and empirical arguments of these texts remain routed through and rooted in the West (Hoepman, 2021; Richards, 2022; Véliz, 2021; Waldman, 2021). Before we situate the experience of privacy specifically within India, we first consider the spatial politics of privacy and how the digital private is political.

Digital private space is political

In creating digital private enclosures for communication – metaphorically referred to by WhatsApp and Meta as the ‘digital living room’ – ideas about informational privacy and spatial privacy become entangled. Informational privacy concerns the protections afforded to the metadata collected on users’ interactions with WhatsApp and with their contacts on the network. Spatial privacy on the other hand concerns the digital architecture of WhatsApp that users ‘inhabit’, where they interact and share messages and media with others and where the content of these personal communications is safeguarded by end-to-end encryption. In addition, users have the option to configure the privacy settings afforded by WhatsApp’s ‘privacy layers’.

The notion of separate private and public spaces or spheres has a particular historical cultural geography conceived of by classical liberal western theorists and in which the home is imagined as a ‘private’ space and the ‘family’ as a privately regulated sphere (Locke, 1690; Rawls, 1971). Feminist and queer theorists have demonstrated how privacy as a spatial practice, has a history of encoding and enabling the persistence of patriarchal and heteronormative power structures where men are presumed to populate the public sphere and engage in public political life while women are confined to the home and domestic matters (MacKinnon, 1989; Pateman, 1989). Feminist critiques have surfaced the ‘darker side of privacy’ and its ‘potential to shield domination, repression, degradation and physical harm to women and others’ (DeCew, 1997, pp 88–89). For instance, Catherine MacKinnon argues that

women are denied power within private spaces and that ‘women have no privacy to lose or guarantee’ (MacKinnon, 1989, p 191).

Meanwhile Carole Pateman suggests that ‘the dichotomy between the private and the public obscures the subjection of women to men within an apparently universal, egalitarian and individualist order’ (Pateman, 1989, p 20). The outcome of these critiques is that women are not autonomous decision makers within the private sphere and that protecting privacy does not protect women. Moreover, with the ‘private or domestic sphere ... held unavailable for public scrutiny’ privacy protection might even be to the detriment of women and children who are subordinate to men in intimate contexts (DeCew, 1997, p 90; see also Blunt and Varley, 2004; Baxter and Brickell, 2014).

Writing in dialogue with these critiques about the Indian context, Kannabiran and Ballakrishnen (2021) document how the ‘public-private dualism has obfuscated, across a range of contexts, questions of difference and discrimination at everyday level’ in India. In post-colonial India the public sphere is constructed through a Hindu majoritarian, patriarchal and caste supremacist lens which depends on ‘the appropriation of female labour, sexuality, and autonomy within the intimate sphere through pervasive asymmetries of power within each of these arenas’ (Kannabiran and Ballakrishnen, 2021, p 761; see also Omvedt, 2003; Fazal, 2016). Consequently, ‘The lines between private and public ... have been of little service to women – especially those navigating law’s periphery – because they delineate, at the core, a set of imagined dichotomies embedded in a structure made without them in mind’ (Kannabiran and Ballakrishnen, 2021, p 1254).

One logical development of these arguments is to jettison the private and the public/private distinction altogether, however others disagree arguing that ‘there is inadequate reason to reject privacy completely based on harm done in private’ (Allen, 1988, p 40 cited in DeCew, 1997, p 90). A more generative feminist critique has challenged the binary distinction between the private and public where ‘the two spheres, the domestic (private) and civil society (public) held to be separate and opposed, are inextricably interrelated’ (Pateman, 1989, pp 121–122, 123). With the boundaries between the private and public blurred, the private, the personal and the home are also recognized as sites of the political and politics (McDowell, 1993).

Notions of the private and public developed a certain way within India’s post-colonial politics. Martha Nussbaum draws on Tanika Sarkar’s research to argue that British colonial rule reinforced Hindu law which grants the household significant autonomy and therefore amplified the notion of male domination over the household. She argues that it was to the British advantage to leave the Indian subject a ‘sphere of self-rule’ and therefore ‘actively assisted in the codification of personal law and the privatization

of marriage and family’ (Nussbaum, 2000). In this context, others have documented how the notion of *ghar* – the home – and *bahir* – the outside or ‘the world’ builds on post-colonial thought which makes visible how the *ghar* as a constructed safe enclosure simultaneously protects women and maintains a cultural space in opposition to the ‘outside’, at once recognized as the western outside and caste/class/racial ‘outsiders’ (Chatterjee, 1993; Gajjala, 2019). While this dichotomy has been critiqued (Legg, 2003), it was crucial both to India’s anti-colonial struggle and the development of cultural Hindu nationalism (Sarkar, 2001). We are interested in how Gajjala (2019) evokes the analytical boundary between *ghar* – the home – and *bahir* – the outside or ‘the world’ – to show how political messaging has become a familiar and sometimes contentious feature of the digital domestic domain, reproducing domestic hierarchies. Gajjala suggests that the WhatsApp group lends itself to forming a private enclosure – the ‘digital *ghar*’ – given the app’s end-to-end encryption and appeal to intergenerational networks.

Research has highlighted the cultural specificities around the gendering of privacy and digital technology in South Asia. For example, Sambasivan et al (2018) document the performative privacy practices that women in South Asia engage in when using mobile phones. They foreground the dissonance between on the one hand ‘the design and development of mobile devices and services’ in which ‘user privacy’ is ‘predominantly modeled on the western experience of “one account, one user” paradigm’ and on the other hand the lived realities of women in their studies who often (willing) shared phones with kin-like relations. All of their participants found innovative ways to maintain their privacy while ‘adhering to cultural values of transparency and sharing that were expected of women’s gender roles’, for example by using app or phone locks, deleting digital traces and content, using private modes and avoiding particular digital activities. Despite all women engaging in privacy-related strategies not all participants recognized privacy as a ‘right’ instead identifying privacy with western values or as something for ‘those rich women’ (Sambasivan et al, 2018, pp 126, 127, 135). The gendered and socially embedded nature of privacy practices on social media is further illustrated in Karusala, Bhalla and Kumar’s research with women in India which shows how women navigated patriarchal norms and privacy boundaries to enable and then protect their participation on social media despite family pressures around respectability (Karusala, Bhalla and Kumar, 2019). These strategies of course echo the kind of ‘privacy work’ that Marwick witnessed among young people in the US.

Exemplifying this ambiguity around the notion of the home as a universally private, safe space, Marwick and boyd argue in the US context that whereas adults might consider the home as a private space, teenagers they interviewed rejected this idea, stating the empirical ways in which parents invaded their personal space such as their bedroom or bathroom and intruded upon

personal conversations with friends. ‘The absence of parents is regularly a key factor for teens to feel as though they have privacy ... When teens explain where they can seek privacy they focus more on who is present than the particular configurations of the space’ (2011, pp 3–4). Marwick’s key argument is that privacy is contextual, it is unevenly experienced and conceptualized and ultimately, ‘the private is political’ (Marwick, 2023).

Not disregarding the possibilities and benefits that privacy can afford to marginalized individuals and collectives, thinking critically about privacy and inhabiting the private demands a sensitivity to the intersectional – everyday and embodied – experiences of privacy and how these are entangled in spatiotemporal relationships of power. For, as Nussbaum concludes,

[t]he private domain is thus defined as a domain in which the powerful have a sway unlimited by considerations of equality and reciprocity ... even when appeals to privacy appear to protect the interests of women (or children), we should be sceptical, and be sure to ask whose interests really are advanced. (Nussbaum, 2000, np)

In Chapter 4, we respond to this contention by examining how WhatsApp as a private digital space that exists beyond public scrutiny has become a site of politics and ‘the political’. In this context we consider the evolving relationship between digital private spaces such as WhatsApp and the quality of democratic practices, online and offline in north India.

Privacy in post-colonial India

In 2017, the journalist Nitin Sethi asked his followers on X (formerly Twitter) to: ‘Please share the equivalent of the word “privacy” in the colloquial versions of the languages you speak’ (Sethi, 2017). This elicited a lively thread with many questioning whether there was a corresponding word for privacy and some suggesting that there was not: ‘This one is a bouncer. I speak 5 languages and can’t think of privacy except in English’ (@apurva_hv), ‘Been thinking. But nothing close in Hindi’ (@anniezaidi) and ‘no perfect equivalent comes to mind for privacy’ (@vi_vibhavjoshi) while someone else pitched in that ‘I don’t suppose Indian languages would have an exact equivalent of this since the concept of privacy is not really something we observe’ (@itssynecdoch). However, people did suggest words that they regarded as adjacent to privacy, such as *gupt* (Hindi: secrecy), *gopniyata* (Hindi: solitude/wanting to be alone), *niji mamla* (Hindi-Urdu: personal matter), *vyaktigat* (liberty), *niji* (Hindi-Urdu: private matter), *neejee baatein* (Hindi-Urdu: personal talks) and *zaati mamlaat* (Urdu: personal matters). The English words private and personal are more commonly used by middle- and upper-class Indians and which reflects the constituency most likely to

interact with Twitter. We further explore situated privacy imaginaries and experiences in [Chapter 7](#).

The ambiguous responses and range of terms suggested as almost equivalents to the English term ‘privacy’ characterize a complex and contradictory relationship to privacy in post-colonial India. On the one hand, discourses prevail that echo the view shared on Twitter/X that ‘privacy is not really something we observe’, often supported by various arguments that indicate a lack of privacy within Indian families or densely populated neighbourhoods and the suggestion that Indians are culturally resistant to the idea of privacy because of strong community identities ([Matthan, 2018](#), p 52; [Sonkar, 2022](#)). On the other hand, arguments and experiences of people challenge the idea that privacy is the preserve of western society and privilege.

Scholars have attempted to recover a longer history of privacy in India. One argument presents privacy in relation to notions of purity and physical space that draws on the writing of ancient Hindu texts. For example, the *Arthashastra*, a political treatise by Kautilya written around 321 BCE indicates concerns with informational privacy given that it provided procedures for ministers of the King to consult in such a way that state policies were not inadvertently leaked ([Goyal and Kumar, 2016](#)). Meanwhile, the *Ramayana*, a Sanskrit epic which narrates the life of Rama and in it, the story of Lakshman Rekha (Lakshman’s boundary) is an example of spatial privacy. Lakshman, the brother of Rama, a god revered by some Hindus, drew a line around their house when both he and his brother were going away. This symbolic boundary was intended to protect Rama’s wife Sita from danger and anyone who crossed the line would burst into flames. Sonkar interprets this story as evidence of the relevance of maintaining personal and spatial boundaries, particularly around the sanctity of the home ([Sonkar, 2022](#), pp 2–4).

Similarities can be drawn between this allegory and the *purdah* system observed by some Hindu and Muslim groups which involves the seclusion of women and adherence to rules around modesty through veiling and the physical separation of genders outside of familial contexts. Drawing on western feminist critiques of the public/private dichotomy discussed earlier, [Kannabrian and Ballakrishnen \(2021\)](#) argue that while the Lakshman Rekha locates privacy within India’s cultural history, it evokes a gendered politics of spatial privacy that legitimizes male authority over domestic space to ensure women’s honour is protected and the home remains sacred ([Kannabiran and Ballakrishnen, 2021](#)).

This gendered politics of privacy puts women under constant surveillance and/or confines them to the private space of the home in the name of their security and family honour. Consequently, a women’s individual privacy is sublimated through the honour of the husband and wider family, a view which informs the Indian courts ongoing refusal to criminalize marital rape

under the Indian Penal Code on the grounds of marital privacy. Moreover, women's uneven experiences of privacy are intersected by caste and religious status, which further complicates the normative idea that privacy is a positive phenomenon in the lives of women (Kannabiran and Ballakrishnen, 2021).

Despite the salience of privacy in India's cultural, religious and political life, privacy was not codified as a fundamental right within Indian law until relatively recently, in response to transformations between the state, citizens, technology and data. Rahul Matthan, a lawyer and public advisor on technology and law in India, documents India's evolving and different 'national experience of privacy' compared to the US and Europe (Matthan, 2018, p 73). Matthan argues that unlike in the US and Europe in the late 1900s, India did not have to confront the same impact of technological shifts and the threat of publicity on personal privacy. However, laws were designed to address concerns about data flows. Under British colonialism, the novelty of the telegraph necessitated the implementation of the Indian Telegraph Act 1885 which granted the government sovereign authority over the right 'to access or control the transmission of personal information'. Rather than protecting Indian subjects' privacy, the law 'allowed the government to order that messages be intercepted, detained, disclosed, or not transmitted for a specific set of reasons' (Chaudhuri and Kang Joseph, 2024, p 157). Matthan contends that since the technology was largely used by the British themselves, the state did not consider privacy as a matter that would affect their Indian subjects (Matthan, 2018, p 48). This reasoning obscures the active role that 'empire's data' and surveillance played in reproducing British domination over Indian subjects and the legacy of colonial apparatus and information infrastructures on privacy today (Arora, 2019c; Isin and Ruppert, 2019). Privacy was a concern for the British colonial administration, but it applied a differentiated approach that protected the private spaces and privacy of some but not others, and in ways that served the interests of colonial rule.

After India became independent in 1947 the Constituent Assembly of India, which was tasked with designing India's constitution, deliberated on whether the right to privacy should be included in the section on fundamental rights. This section was to include rights that would be justiciable in nature, that is citizens could go to court if those rights were to be violated. The chairperson of the Constituent Assembly, Dr B. R. Ambedkar wrote:

The right of people to be secure in their persons, houses, papers and effects against reasonable searches and seizures shall not be violated and no warrants shall issue but upon probable cause, supported by oath of affirmation and particularly describing the place to be searched and the persons or things to be seized. (cited in Matthan, 2018, p 54)

Ambedkar was therefore in favour of ensuring that Indian citizens' privacy was not threatened in the name of state security. However, this was precisely the reason why some members of the drafting committee objected to including it in the list of fundamental rights. Alladi Krishnswamy Aiyar and Benegal Narsing Rau argued that making privacy a fundamental right would make the 'administration of justice' difficult. They feared that the right to privacy would be invoked to prevent searches and other forms of surveillance (Matthan, 2018, p 55). Despite such deliberations, the right to privacy was removed from the list of fundamental rights in the draft of the Indian Constitution. The final constitution tipped the balance between personal privacy and criminal justice in favour of national security and state surveillance. Though claims to individual privacy were variously asserted in court cases following India's independence, the ultimate judgements tended to support the state's right to carry out surveillance against those suspected as criminals and the prevailing power of the state to protect state security typically triumphed (Matthan, 2018; Kannabiran and Ballakrishnen, 2021).

The introduction in 2011 of a government biometric technology for collecting and processing personal information – the Aadhaar card – proved to be a watershed moment in transforming privacy into a public matter for India's citizens. The Unique Identification Authority of India (UIDAI) is the body responsible for distributing Aadhaar identity cards to all residents of India. Acquisition of an Aadhaar requires citizens to submit their biometric data including a scan of their fingerprints and retinas. A citizen's demographic data is linked to a 12-digit identity number and stored in a centralized database. Although on paper Aadhaar is not strictly mandatory for citizens, the government has progressively made it a requirement for citizens wishing to access welfare schemes such as subsidized food and guaranteed labour. In 2016 the government introduced the Aadhaar Act and launched its associated digital identity platform. This was also subject to further legal challenges.

The public-private scheme provoked debates about whether Aadhaar violated an individual's privacy and raised concerns about who owns, protects and controls the personal data of 1.3 billion Indian citizens. The very existence of the Aadhaar 'platform' presented the possibility of linking personal information with banks, telecom companies, hospitals and schools to understand population and individual level behaviours concerning communications, finance, education, health and much more (Sudhir and Sunder, 2020). Reflecting the concerns of civil society and privacy activists' Justice K.S. Puttaswamy, a retired judge of the Karnataka High Court, had earlier filed a writ petition in 2012 in relation to the Aadhaar project that challenged the constitutional validity of the Aadhaar databases. He objected to the inadequate privacy safeguards in place to ensure the security of the data along with a lack of checks on the power of government to use the

biometric data it collects. And he also challenged the mandatory requirement of an Aadhar card for all citizens seeking benefits from the state.

Nitin Sethi had posted his question on Twitter in 2017 inviting vernacular words for privacy just a few months before India's Supreme Court finally heard Puttaswamy's case on whether the 'right to privacy' was a fundamental right under the Indian Constitution. After a lengthy journey through the Indian courts the case was placed before a Nine Judge Bench of the Supreme Court for a final verdict on 24 August 2017. The bench unanimously recognized that privacy *was* 'a distinct and independent fundamental right under Article 21 of the Constitution' which was enforceable and multifaceted. Under this ruling the right to privacy pertained to 'the body and mind and included decisions, choices, information and freedom' (SCO, 2017c).

In 2018, a further case determined the constitutionality of the Aadhaar Act where the majority opinion was that the Aadhaar Act was not violative of the fundamental right to privacy established by the Puttaswamy case. The court reasoned that Aadhaar would be an efficient and transparent means to distribute welfare and the Aadhaar Act which created provisions for this, was not unconstitutional. However, certain individual provisions of the Act were struck down including the compulsory linking of Aadhaar with bank accounts, collection of citizens' metadata conducive to a surveillance state, and enabling private entities to use Aadhaar for service delivery. Moreover, Justice Chandrachud dissented on multiple grounds and held that Aadhaar was in fact a violation of privacy as it is violative of 'informational privacy, self-determination and data protection'. He urged that a strong regime for the privacy protection and safeguards in line with that provided under the EU's GDPR was required to give Aadhaar legitimacy and instil public trust (SCO, 2018).

The Puttaswamy judgement was a landmark moment, but rather than closing discussions about the right to privacy it sparked new ones concerning the implications of a right to privacy for data and informational privacy. Until then, information transmitted by computer resources was regulated under an amended Indian Telegraph Act in conjunction with the Information Technology (IT) Act, 2000 and the Information Technology (Amendment) Act, 2008. The provisions of the latter acts were modelled around the colonial Indian Telegraph Act and reflected an increase 'in the government's appetite to exercise their sovereign powers to access private communications' (Chaudhuri and Kang Joseph, 2024, p 158). The amendment to the IT Act in 2008 responded to the demands of global companies who outsourced their IT and customer service to India and sought reassurance about the protection, storage and transfer of sensitive personal data in the absence of a formal privacy law in India (Matthan, 2018, pp 116–117). The amendment legislated for compensation and/or punishment in cases of privacy breaches to personal data obtained

under lawful contracts. While protecting the integrity of personal data held by companies operating in India, the amendments also expanded the government's sovereign powers to both monitor and order the decryption of data. A further set of rules were created by the government in 2011 under the IT Act which permitted the transfer of personal sensitive data within India and across its borders with the consent of the user and to meet contractual obligations (Chaudhuri and Kang Joseph, 2024). However, these were merely edits to existing Acts and did not amount to a comprehensive regulatory framework designed to protect India's personal data and privacy.

It was only in 2017 that the government commissioned a report to explore how data privacy and protections could be more comprehensively regulated under the law. Assigned just a month before the Puttaswamy judgement and led by the retired Supreme Court Judge Justice B. N. Srikrishna this report became the basis for a new Data Protection Bill. Recognizing India's post-colonial position, it stressed that one of its goals was to be *the* framework for data regulation in the global south acknowledging the need for personal data protection but not at the expense of India's economic growth. After various iterations, the Indian government passed the Digital Personal Data Protection Act (DPDP) in 2023 and at the time of writing its draft rules are under consultation.

The privacy fault lines created by India's weaker privacy and data protection standards mean 'the techno-oligarchs such as Facebook, Twitter, Amazon, and Google are computing data of much of this region' (Arora 2019a, p 368). Arora contends that the expansionist outreach of pervasive datafication of the 'peripheries' by the 'core' can be viewed as a 'colonial impulse' (Dourish and Mainwaring, 2012, p 135 cited in Arora, 2019a). By documenting WhatsApp's evolving privacy policies and the litigation surrounding these updates in India, Chapter 5 examines how WhatsApp (and Meta) productively negotiates and exploits global data privacy inequalities and, moreover, how the Indian government, civil society and citizens have variously negotiated and critiqued Big Tech's 'expansionist' tendency. The shifting relationship between technology and privacy in India calls into view how various 'things' – the telegram, computers, Aadhar card – interacted with shifting privacy discourses and relationships across scale.

Sensing privacy

A feminist geopolitical approach to privacy learns from the materialist turn in feminist geopolitics (Dittmer, 2014; Dixon, 2015; Sharp, 2021). This prioritizes the significance of not just the everyday experiences of people and representations but also of sensing privacy through the 'privacy things' that constitute privacy architectures: data, code, passwords, smartphones, apps, terms of service contracts and legal documents. Moreover, it highlights

how these ‘things’ are configured and represented through Big Tech, state and everyday performances in ways that give meaning to this materiality (Sharp, 2021). Scholars have long argued that (digital) technologies have material and political lives, and that technology shapes the social, as much as the social shapes technology (Heidegger, 1977 [1954]; Winner, 1988; Haraway, 2004; Wajcman, 2004; Sharp, 2021).

Attempts to classify internet architectures usefully foreground the more-than-human nature of the internet and more-than-representational (Lorimer, 2005). A feminist geopolitical approach to privacy includes ‘people and things’ and endeavours to ‘recognise the ways in which the things are brought into the political; through debate, challenge, argument’ (Sharp, 2021, p 995). It thus combines ‘an attentiveness both to political representations and to practice’ (Sharp, 2021, p 991). And seeks to understand these with respect to the ‘digital mundane’, that is the ‘on-the-surface, taken-for-granted, seemingly ordinary and routine sites, objects, data productions, and networked practices of everyday life’ (Leszczynski, 2020, p 1151). Our focus on WhatsApp’s privacy architectures therefore centres human and non-human relationships and the politics of ‘privacy things’ through an openness to contradiction, ambiguity and complexity. To do this we build on ‘domestication’ theories which afford an analytic for examining the situated and relational materiality of ‘privacy things’ in three interconnected ways. Here ‘domestication’ speaks to both the constructed divisions between the public and private and how these underpin political and economic agendas both within the domestic and international (Brickell, 2012; Woodyer and Carter, 2020; Jackman and Brickell, 2022).

Feminist geopolitics confronts the perceived dichotomy between geopolitics and the public sphere on the one hand and the private sphere and everyday life on the other hand by focusing ‘on the entanglements of power rather than a binary between them’, captured in the notion of the ‘intimate global’ (Mountz and Hyndman, 2006b; Brickell, 2012). Building on Woodyer and Carter (2020), Jo Sharp argues that the concept of ‘domesticating’

draws our attention to the ways in which divisions between public and private are inscribed on the international-domestic political landscape in the same ways in which public-private is inscribed into the everyday: the dangers of the public/international are set against the protection offered by patriarch/state in the domestic spaces. (Sharp, 2021)

Moreover, as Woodyer and Carter put it, domesticating geopolitics foregrounds how the ‘entangled relation of proximate and distant occurs through embodied and affective modes of interaction’, not just how the geopolitical plays out in ‘the domestic’ (Woodyer and Carter, 2020, p 1069).

Second, recognizing ‘the embodied materiality of humanity that links us to the rest of the world’ (Dittmer, 2014, p 389), ‘domestication’ concerns how and why digital technologies become domesticated in practical and symbolic, anticipated and unanticipated ways (Silverstone, 1994; McDonald, 2015; Gajjala, 2019). Domestication theory recognizes the ‘double articulation’ of technology, that is, that technology is not only meaningful in and of itself, but also as a carrier of meaning (Morley and Silverstone, 1990, p 48). Moreover, it accounts for how people negotiate and renegotiate their relationship with technologies including their values and attitudes and as McDonald proposes, how technologies mediate or affect social relations too (McDonald, 2015). Finally, ‘domesticating’ also speaks to how WhatsApp and Facebook/Meta has advanced the imaginary of the ‘domestic’ to translate or vernacularize abstract technical concepts – such as digital private space or end-to-end encryption – into everyday life as we explore in Chapters 6 and 7. How and why WhatsApp and its digital private spaces are attributed meaning within Menlo Park, California, and how that meaning is circulated, negotiated and renegotiated by citizens, lawyers, journalists, the Indian government and WhatsApp in other contexts, is an important dimension of this book.

Privacy as tonic: the promise of privacy and colonizing private futures

As we indicated in the introduction, technological imaginaries are political. They are also geopolitical. Mark Zuckerberg’s prophecy that the ‘future is private’ pitched privacy and private digital messaging as a ‘tonic’. In other words, as the technological solution for more trustworthy and authentic communication and the antidote to Facebook’s reputational hit over its untrustworthy use of public data. In an uncertain, future-orientated society, scholars have examined the importance of future imaginaries for understanding and influencing shifting social, technical and economic dynamics (Jasanoff and Kim, 2015; Beckert and Bronk, 2019). Optimistic visions of technological progress and change have been central to technoutopian discourses. Techno-optimist imaginaries function to legitimize change. Evoking the inevitability and desirability of that change in the face of crisis or stasis, techno-optimism also has a moral politics that underscores the belief that ‘technology plays a key role in ensuring that the good prevails over the bad’ (Danaher, 2022, p 26).

The anticipation of a better future is accompanied by an obliviousness for how technology is ‘embedded in the real history of real people, real desires, a real economy and real political possibilities and foreclosures’ (Carey, 2005, pp 446–447) and has been mobilized as ‘a powerful political and cultural weapon’ (Carey and Quirk, 1989, p 134). Through his analysis of Zuckerberg’s utterances up until 2017, Haupt (2021) demonstrates how

‘Facebook’s future imaginaries’ have been intentionally and discursively constructed over the lifetime of the product (see also [Hoffmann, Proferes and Zimmer, 2018](#)). He argues that Facebook’s future imaginaries are a ‘strategic resource’ that grant Facebook ‘corporate legitimacy’ and strategically position the company ‘as a valuable social actor’ (see [Gillespie, 2010](#); [Haupt, 2021](#), pp 238, 239). Curious about Silicon Valley’s philosophical foundations, Adrian Daub has excavated the origins of ‘what tech calls thinking’ to understand the relationship between Silicon Valley products and the narratives or ‘reframing’ that make them ([Daub, 2020](#)). Examining not so much what is said but what lies beneath the narrative helps to understand ‘how the changes Silicon Valley brings about are made plausible and made to seem inevitable’ ([Daub, 2020](#), p 4). Daub draws on the journalist Franklin Foer to make the point that Silicon Valley companies ‘have a set of ideals, but they also have a business model. They end up reconfiguring your ideals in order to justify their business model’ ([Foer, 2017](#) in [Daub, 2020](#), pp 3–4).

Building on the work of [Hoffman, Proferes and Zimmer \(2018\)](#) and [Haupt \(2021\)](#), we consider the discursive work of Facebook’s ‘privacy futures’ – and ‘privacy histories’. We explore how this discourse is constructed and articulated as a form of ‘corporate prophecy’ that engages investors, employees, users and governments in order to ‘strengthen’ Facebook and WhatsApp’s ‘position in a future-oriented society’ while also deflecting attention from the company’s aspiration for data, power and profit ([Haupt, 2021](#), p 239). We build on Haupt’s argument that Facebook’s future imaginaries function to ‘colonise the future’ and play a key role in legitimizing and reproducing its global project of ‘data colonialism’ ([Haupt, 2021](#), p 238). Just as Ziaduddin Sardar asks of ‘future studies’, it is important to question *who* is imagining the future and *for* who, in the case of WhatsApp and Big Tech more broadly ([Sardar, 1993](#))?

Reading privacy stories

Privacy Tectonics draws from several qualitative projects that employed a multi-sited and multi-method approach to understanding situated and entangled geopolitics of privacy beyond western institutions and individuals in this book. Drawing on digital ethnographies, participant observation and interviews carried out by a team of researchers and the authors between 2019 and 2024, we focus on stories that people tell us and themselves about privacy. Ordinary citizens, political party workers, civil society activists and journalists in India narrated their experiences of WhatsApp, digital private messaging, and how they think about privacy. The research was conducted in north India and primarily in and around the capital, New Delhi. The project actively engaged with participants from a diversity of backgrounds along the lines of religion, caste, age, sexuality and gender, in the manner

in which they described themselves. With the empirical research largely in New Delhi, the majority of interviews were in Hindi and/or English, and as such reflect a particular view on India and on privacy. We urge further research on the situated politics of privacy in other regions and particularly in more rural contexts to build on and critique this work.

Interviews and ethnographic research are read alongside the stories that Meta, India's legal system, and the Indian government narrated about privacy. To understand these, we analysed Meta's financial reports; WhatsApp and Facebook website archives, their terms of service, privacy policies and blogs; legal documents, the Indian Constitution; Indian government policy, web content and press releases; media interviews given by Facebook and WhatsApp as well as other technology executives; and civil society reports. A more detailed overview of the research methods, participants and the materials we analysed is available in the Appendix.

The Politics of Digital Private Messaging

Nitya was a university student in New Delhi from a middle-class Hindu family. In early 2019 she decided to leave her extended family WhatsApp group. Her primary motivation for this decision was that she could no longer abide the volume and toxic tone of political messages that were being circulated by her family members. She described her relatives as Hindu ‘right-wingers’ who supported the main ruling party, the BJP, led by Prime Minister Narendra Modi. They revelled in the opportunity afforded by cheap data packages to forward hundreds of memes, messages and videos each day, that were typically pro-Modi, and often anti-Muslim in their content. Portraying herself as ‘politically neutral’, Nitya explained the negative impact that the messages had on her wellbeing, and how she did not want to wake up every day to yet more hate messages, which would undoubtedly intensify with the forthcoming national elections. After discussing her stance with her mother, both agreed that any attempt to counter or question the offensive WhatsApp messages and ‘fake news’ forwards would be futile. Moreover, it would likely reinforce her relatives’ political ideology and simultaneously risk herself being framed as anti-Modi and therefore as ‘anti-national’. Given the perceived obstacles to engaging in meaningful political dialogue in the extended family WhatsApp group, Nitya felt not only exhausted and distressed by the endless circulation of online extreme speech but also excluded from this private digital space.

Private digital spaces afforded by WhatsApp are central to everyday ‘political talk’ in India (Valenzuela, Bachmann and Bargsted, 2021). Digital spaces are inextricably woven into our everyday practices of consumption and communication, work, play and politics (Gerbaudo, 2012; Nyabola, 2018). As part of people’s everyday lives, in India, WhatsApp is where many political conversations take place by way of forwarded messages and memes, and it is deployed by political parties for political communication too. Political participation in India is high, with voter turnouts close to 70 per cent, and the

poor voting more than the rich (Banerjee, 2014). Participation now extends to WhatsApp in the form of one-on-one conversations, communication within personal groups, publicly accessible groups that one can join with a weblink, and public channels and communities. Content also circulates between the private and more public digital spaces on the same app. For example, both private family groups like Nitya's and more public WhatsApp channels run by news organizations have political content circulating. By focusing on WhatsApp in everyday political life we shift the emphasis away from normative western concepts of what democracy 'should' look like to 'the ways in which values and practices of democracy become embedded in particular cultural and social practices' (Michelutti, 2007, p 639). The 'social imaginaries' of democracy in India influence how WhatsApp might be mobilized for politics (Banerjee, 2021).

In this chapter, we argue that the shifting geopolitics of digital privacy and WhatsApp have become intertwined with democratic politics in India. We examine the question: how have WhatsApp's private digital messaging spaces transformed politics and democracy in India and vice versa? We argue that WhatsApp contributed to India's democratic erosion amidst the rise of Hindu nationalism in contemporary India. In making this argument, we temper the enthusiasm of scholars who see private digital spaces as contributing positively to democratic politics (Papacharissi, 2010). WhatsApp is reconfiguring democracy in different ways, first, through the creation of private digital spaces that allow for anonymized extreme speech and mis/disinformation on subterranean or hidden digital storytelling infrastructures. As the BJP and other political parties mobilize social media platforms to communicate and campaign, political conversations that typically took place at tea stalls, street corners and living rooms, now also take place on smartphones and social media platforms. WhatsApp's subterranean storytelling infrastructure has proven to be efficient at circulating Hindu nationalist digital content at speed and scale within new and existing societal and political networks and away from public scrutiny where the source of messages cannot be traced (Chakrabarti, Stengel and Solanki, 2018; Williams et al, 2022). Hindu nationalist messaging encapsulates satirical as well as violent content, activating feelings rather than prioritizing facts, to polarize political imaginations (Udupa, Gagliardone and Hervik, 2021) and make affective appeals to readers (Papacharissi, 2014). The messages often rely on mis/disinformation too. Disinformation also circulates in closed groups on Facebook, which often escapes scrutiny and remains online due to Meta's privacy protections (Ong, Tapsell and Curato, 2019, p 15). But WhatsApp's encrypted digital spaces make a subterranean private network more readily available to the Hindu right in India.

Second, WhatsApp has become critical to political communication by political parties. Messaging that circulates in private takes on public qualities

and public messaging during campaigns also circulates in private networks. We document how political messages on personal networks appeal to people's emotions to gain support for ideological projects such as right-wing Hindu nationalism. We show how these digital 'political economies of feelings' (Fortier, 2010) are shaped by the articulation and defence of 'truths' which find traction through WhatsApp and increasingly determine the contours of sociodigital inclusion and exclusion.

Third, where political communications and conversations on and around WhatsApp groups (re)produce boundary making we examine how sociodigital frictions arise along these boundaries. Nitya, for instance, was not allowed to disagree with elders on the extended family group while exiting the group was deemed a risk to family unity. The patriarchal and familial hierarchies and silences created friction between intimate relations, or frictive intimacies. People spoke about how negotiating frictive intimacies within WhatsApp groups had broader implications for questions of identity and belonging that challenged imagined boundaries between public and private or digital and physical life.

Fourth, by examining the life of a neighbourhood WhatsApp group, the chapter reveals how digital private messaging networks were mobilized during the COVID-19 pandemic to create spaces of middle-class care and concern while also cultivating authoritarian tendencies. Grassroots authoritarianism found expression through the disciplining of lower-class and minority bodies and the surveillance of all which extended beyond the COVID-19 lockdowns. For religious minorities, middle-class neighbourhood WhatsApp groups were a microcosm of Hindu nationalist politics, the dynamics of which contributed to their experiences of unbelonging and the unmaking of citizenship. Finally, we explore the conflicting politics of WhatsApp's digital private spaces by examining how Narendra Modi, the Bharatiya Janata Party and Hindu right supporters have exploited WhatsApp's subterranean digital storytelling infrastructures for political mobilization and campaigning and how, when in power, the central government has adopted WhatsApp as a formal (and informal) technology of governance. As a core political infrastructure WhatsApp serves as both a digital private and public infrastructure.

Digital private spaces and democracy

New spaces for politics

The relationship between digital private spaces and democracy has evolved with the changing nature of the digital private spaces that politicians and citizens mobilize for democratic politics. Writing about internet-enabled private spaces, Zizi Papacharissi (2010) has argued that 'online technologies afford us spaces, public and private, rather than a public sphere' (Papacharissi,

2010, p 127). Moving away from a simple techno-utopian or technodystopian view of digital media with respect to democracy, she urges us to focus not on whether technology is democratizing but on ‘the reorganization of space that technology permits’ and how new media transforms and is transformed by social relations (Papacharissi, 2010, pp 3, 7). Challenging normative theories that claim that democratic life is realized in the public sphere (Habermas, 2005), she shows that new digital private spaces become active sites of political life and citizenship by enabling new possibilities for civic connections and dissent (Papacharissi, 2010, p 167). Drawing on examples from the US, Papacharissi shows how individuals attempted to counter their sense of powerlessness within a contemporary democracy by participating in online discussion forums, blogging and voting in online polls. She writes that this sense of powerlessness had resulted in declining voter turnout but participation in new spaces of the internet which ‘expand information and opinion exchange’ for those who have access and the required literacy levels (Papacharissi, 2010, p 20). For her, the private sphere of the internet restores power to the individual and often leads to newer ‘civic tendencies’ (Papacharissi, 2010, pp 20–21).

In India, where voter turnouts have been on the rise rather than decline, private digital spaces are an additional arena for political participation rather than a panacea for declining participation by citizens. In 2011, middle-class Indian citizens widely participated in an anti-corruption movement through internet forums, citizen journalism and TV news polls centred around the ‘*aam aadmi*’ (common man), the movement gave rise to a new political party and brought down the incumbent Congress-led UPA government in the 2014 election (Udupa, 2014). In the pre-smartphone days, citizens turned to the internet and blogs for civic action as described by Papacharissi. This moment of internet activism in India coincided with global protests such as the Arab Spring and Occupy Wall Street. Civic duty through protest had become popular. However, online activism was only one small part of the repertoire of political action in India. Since unlike the US, voting rates are high in India (68 per cent in the 2024 national election), people are much more involved in political conversations and actions at the grassroots (Banerjee, 2014). Their ‘civic tendencies’ have not relied only on new media, even as digital media may have bolstered such tendencies.

Papacharissi (2010) also contends that internet-enabled private spaces are new democratic arenas for citizens to participate in politics by expressing dissent, and by thinking differently. But she does provide a word of caution:

It is possible that we have created technologies that have a social and political place within a democracy, but do not inherently make democracy better. Therefore, it might make sense to frame these

affordances [blogs, online citizen polls etc.] as democratic, but not democratising and online spaces also end up reflecting the inequalities present in the public sphere. (Papacharissi, 2010, p 144)

While the digital private spaces of WhatsApp are somewhat different to blogs, we build on Papacharissi's caution and contend that intimate private digital spaces have contradictory relationships with democracy – at times eroding it, and at times strengthening it. The virality, veracity and volume associated with WhatsApp messages make it an effective tool for political messaging. While it enables political actors to reach out to a large number of people with campaign messages, it also allows for misinformation and democratic decline (Banaji and Bhat, 2019; Williams et al, 2022). The volume of political content that can be circulated on private digital spaces of WhatsApp, alongside the reach of this content in people's personal groups and networks has meant that political parties and other interest groups weaponize the medium for propaganda, dividing people and influencing political opinions and choices (Singh, 2019). Together with other digital media platforms, WhatsApp is shaping the global turn towards right-wing populism, especially 'digital populism' in our times (Cesarino, 2019).

WhatsApp's digital private spaces

Our focus is on how political party actors, activists and ordinary citizens use WhatsApp to generate, forward, engage with and even ignore messages with political content, and what these acts mean for rights, freedoms, dissent and inclusion. Smartphones and digital messaging apps have created additional spaces of political conversation and participation, enabling political activities through WhatsApp: party politics, political campaigning and activism. Previously, only literate citizens with access to desktop computers could blog or act as citizen journalists, whereas the spread of smartphones, cheap data packages and voice/video communication has brought many more Indians into digital-political spaces. WhatsApp only needs a smartphone and can be used even by those who are not literate. As Fabiha, a migrant domestic worker from Bengal, told us in Delhi, 'Others save their numbers on my phone and I can open them on WhatsApp and identify them through their display pictures. I cannot read and write, but I can watch and forward videos and send and receive voice notes.' WhatsApp's features thus make it easier for political content to circulate despite lower literacy levels.

Such widespread use of WhatsApp makes it a potent tool for political processes across the global south. Research projects on political parties in Malaysia, Brazil, Columbia and Kenya, found that because WhatsApp has more penetration and the message appears to come from a known and reliable source, WhatsApp is given a central role in political campaigning (Rennó,

2018). Across Asia, Africa and South America, bulk political messaging on WhatsApp is deployed in political campaigns with the help of an army of party workers and volunteers, as seen especially in India, Brazil, Nigeria and Indonesia (Hitchen et al, 2019; Johns, Matamoros-Fernández Baulch, 2023). WhatsApp connects voters with their candidates and parties more directly, but the use of WhatsApp in political campaigning always comes with concerns about mis/disinformation, mobilization of digital private spaces to elect and entrenchment of right-wing/authoritarian leaders. In Brazil, for example, WhatsApp is used far more by right-wing politicians (Rennó, 2018).

While WhatsApp strengthens the reach of opposition parties and gives women and young people new opportunities to participate in politics on the one hand, on the other hand, WhatsApp emboldens ‘candidates and their supporters to spread “fake news” – whether inadvertently (misinformation) or deliberately (disinformation)’ (Cheeseman et al, 2020, p 147). Part of the appeal of WhatsApp for political messaging lies in its ability to target people’s emotions. The intimate and personal nature of communications on WhatsApp groups can induce emotional affects that structure feelings of nationalism, belonging and identity (Chakrabarti, Stengel and Solanki, 2018; Oza, Williams and Kamra, 2024). Such feelings can both strengthen democracy by bringing people together, but they can also create exclusions and further marginalize minoritized communities. As discussed earlier, affect produced through WhatsApp’s storytelling infrastructure presents ‘a way for understanding both the opportunities for voice that networked platforms invite, and the inequalities in expression that they frequently conceal or reproduce’ (Papacharissi, 2014, p 27). The emotions produced through storytelling in WhatsApp’s networks gives voice to certain political opinions while sidelining others.

WhatsApp’s role in politics also creates digital publics through the deployment of digital private spaces for politics. For the most part, WhatsApp can be described as a private and semi-private digital messaging app which people use for one-on-one conversations with their contacts or to communicate on the WhatsApp groups they share with family, friends, neighbours, colleagues and acquaintances. However, WhatsApp additionally introduced larger groups of up to 1024 members (earlier a group could only have 256 members) and features including ‘Communities’ and ‘Channels’, which enable sharing information with those beyond one’s personal contacts, while still being private. Some scholars have documented how ‘Communities’ and ‘Channels’ represent new ‘WhatsApp Publics’ which contribute to a ‘public forum that plays an important role in the formation of public opinion’ (Johns, Matamoros-Fernandez and Baulch, 2023, pp 104, 105). WhatsApp forms ‘publics’ or ‘communities’ by connecting not just contacts, but also strangers (Johns, Matamoros-Fernandez and Baulch, 2023, p 106). Duncan Omanga (2019) writes about the generative possibilities of WhatsApp in

Kenya for participatory democracy and the emergence of ‘digital publics’ that are formed on and through political discussions taking place on WhatsApp groups. Such groups are formed specifically for discussing the government’s failings and what can be done to bring about change. He sees the emergence of publics here because there is a conscious effort by a group of citizens to talk about politics. Discussions such as these are facilitated by the closed and private nature of WhatsApp where citizens feel safe enough to criticize their government with people they know and trust. Thus, the emergence of ‘digital publics’ in such a context is dependent on WhatsApp’s private digital spaces. So while WhatsApp has introduced features that afford more public forms of communication, its popularity as a tool for politics originates in its private or encrypted digital messaging spaces (see [Williams et al, 2022](#)). In practice, there are degrees of privacy and publicity on WhatsApp groups, and channels and communities are now an integral part of the app, but unlike Facebook (or X), WhatsApp is not a public messaging board. WhatsApp is a privatized digital enclosure. While it might sometimes mirror other social media platforms, it operates differently due to the encrypted, subterranean nature of its digital spaces. We consider WhatsApp’s role in politics accordingly, placing it within the debates on private digital spaces and how those impact democracy today, from their use for activism to everyday politics of silence and resistance, and from party-political campaigning to affective grassroots appeals to nationalism.

WhatsApp’s intimate private spaces simultaneously facilitate political participation and activism while also contributing to democratic decline. WhatsApp enables activists and dissenters to organize. Take the example of activist coordination; WhatsApp allows for ‘backstage activism’ beyond the scrutiny of governments as opposed to the frontstage activism of public social media ([Treré, 2020](#)). This is especially useful when governments or authoritarian leaders control print and broadcast media. Writing about movements in Mexico and Spain, [Treré \(2020\)](#) shows that activists are often paranoid and anxious about being visible as protestors on Facebook and X (formerly Twitter) as they might face negative consequences. In such a situation, WhatsApp functions as a relatively safer space to connect with like-minded people. In Malaysia too, activists considered WhatsApp a safe space after the government in 2013 began to arrest activists who were vocal on Facebook and Twitter ([Johns, Matamoros-Fernandez and Baulch, 2023](#), p 104). WhatsApp’s end-to-end-encryption ensured their security in an environment of widespread state surveillance. They saw WhatsApp as a platform that provided private as well as semi-public groups for discussing politics and coordinating political action. As a ‘backstage communicative tool’, WhatsApp ensured effective political organizing ([Treré, 2020](#)).

But over time, WhatsApp’s privacy updates and government scrutiny of WhatsApp chats impacted the perception of WhatsApp as a safe and

secure digital space. Activists in Malaysia no longer consider WhatsApp a safe space for activism (Johns, Matamoros-Fernandez and Baulch, 2023). But they were unable to move their activities away from WhatsApp after Facebook acquired it and there were talks about more compromised privacy settings. Some of them wanted to shift to Telegram but could not leave WhatsApp as it was the most popular messaging app among people there (Johns and Cheong, 2021; Johns, Matamoros-Fernandez and Baulch, 2023, p 117). In India, student activists such as Sabeena (introduced in Chapter 1), were wary of using WhatsApp after the police began to seize activists' phones and physically access WhatsApp chats, as we discuss in more detail in Chapter 7.

WhatsApp in Indian democracy today

WhatsApp is a part of the everyday lives of Indians and features prominently in popular culture too. The significance of WhatsApp within 'political talk' in India was noticed and amplified by the prominent Hindi media journalist Ravish Kumar. Kumar left the private news channel, NDTV, after it was bought over by Gautam Adani, among the richest Indian businessmen who is close to Modi. Kumar started a YouTube channel, and, in his videos, he often refers to 'WhatsApp Uncles'. In one such video right before the 2024 national parliamentary election, he asked viewers to wake up and see the problems with the incumbent government and not believe 'WhatsApp uncles' who say '*sab accha hai*' (all is good) despite opposition leaders getting arrested (Kumar, 2024). It was Ravish Kumar who had earlier satirized WhatsApp's reputation as a messaging app for spreading mis/disinformation by popularizing the term 'WhatsApp University'. Those calling out their friends and family for parroting and forwarding false information often ask: Did you learn this at WhatsApp university? All in all, there is no election in India now without either the use of WhatsApp or people discussing how it is a medium for spreading 'fake news' (Chakrabarti, Stengel and Solanki, 2018).

Fake news is a term that covers both misinformation and disinformation. The culture of sending forwards among Indians makes it possible for political content generated by political parties to be circulated widely and for mis/disinformation to travel across WhatsApp groups (Chakrabarti, Stengeland Solanki, 2018, p 26). Some examples of political mis/disinformation we came across are false accusations about opposition politicians colluding with enemy countries, incorrect information about Modi improving India's global standing, and made-up theories about the Muslim minority purposefully working to increase their population to overtake the Hindu majority population. Extreme speech against the Muslim minority population is also common. Messages containing mis/disinformation and extreme speech

originate from both political parties and citizens. Political parties connect with citizens through WhatsApp groups and channels. They mobilize WhatsApp's private digital spaces during elections and beyond to forge intimate connections with voters and enable micro-targeting.

WhatsApp's efficacy in making messages viral across people's personal networks differentiates it from more public digital platforms like X (formerly Twitter) and Facebook. This effectiveness derives primarily from the sheer number of people who use WhatsApp in India. With over 500 million users, the reach of WhatsApp to even the most remote parts of the country makes it the preferred digital platform for political parties and citizens alike (Garimella and Eckles, 2020; Jaswal, 2024). Moreover, as a 'technology of life' (Cruz-Moya and Harindranath, 2020), WhatsApp is woven into the digital-social fabric of people's lives. Staying in touch with loved ones, ordering groceries, fixing appointments and even contacting doctors are increasingly done on WhatsApp. The pervasive presence of WhatsApp in people's lives makes it an effective tool for political messaging. Finally, the intimacy and trust afforded by WhatsApp means people are more likely to believe in and forward the messages they receive as they usually come from a trusted source such as a family member or a friend (Chakrabarti, Stengeland Solanki, 2018).

WhatsApp is mobilized by all political parties for campaigning and storytelling around political projects in India. But the ubiquity of WhatsApp in political communication has corresponded with the rise of Narendra Modi as a populist right-wing Hindu nationalist Prime Minister in India (Ali, 2020; Jaffrelot and Verniers, 2020). The BJP was the first to exploit the potential of digital private spaces for communicating both within the party and directly with its voters.

We found that a large volume of WhatsApp messages advocated for Prime Minister Modi, voting for the BJP, and supporting Hindu nationalism. Messages also incited emotions of fear, anger and hatred among supporters of the BJP's politics against minorities and the party's political opponents. These messages circulated away from public scrutiny in WhatsApp's private spaces and created an atmosphere where voters received messages that reinforced dominant political ideas. It must be added that the BJP and its affiliate organizations have in the past relied on other forms of media to seek supporters for their project of casting India as a Hindu nation (Rajagopal, 2001). Mobilizing the internet for political power is just the latest iteration of the Hindu right's influence within and through the media landscape.

The BJP's IT cell was well established prior to the party's 2014 victory. Having attracted the expertise of return migrants from Silicon Valley, it understood the power of large data sets and social media to target and mobilize voters through populist and polarizing political messaging initially with Facebook, then Twitter and then WhatsApp. The entry of political

consultants also revitalized the media strategy of parties. The IT cells and consultants who worked at this ‘backstage of democracy’ included WhatsApp in the digital campaigning strategies of political parties (Sharma, 2024). As an ex-political consultant of the BJP writes in his exposé on the BJP’s election strategies, in WhatsApp the BJP ‘found a new weapon that offered much better targeting than Facebook ever could’ (Singh, 2019).

For the BJP, tapping the power of the digital was especially important for accessing undecided voters beyond the public reach of political party workers and volunteers. As Vaibhav, a BJP worker told us,

[It’s] very very important. I think that because you see, people are not coming out. People are not speaking. It’s only through social media that you can reach out to the neutral voters. In your meetings only Congress men are coming. In BJP meetings, only BJP guys are coming. To reach out to the neutral voters, the best medium is social media. And people no longer spend time with their family, with their girlfriend, with their wives, but instead spend time with their phones. The first thing they do every morning is check their phones. The last thing they do before going off to sleep is ... check their phone. So ... we have to get inside their phones. And they have developed that appetite. So, if you don’t give them the content, otherwise someone else will give them the content.

The BJP has exploited the potential of digital private spaces of WhatsApp to create intimacies both *within* the party, among its workers, and with the voters. As a political consultant for the BJP recounted in an interview with us, WhatsApp was also extremely effective at producing cohesion within the party, by connecting volunteers ‘even at the lowest level’ and nurturing a sense of intimacy across the hierarchies so that they ‘feel that they are part of the inner workings of the party ... and privy to the meetings and private spaces of the party’. WhatsApp therefore mediates new digital party-political intimacies between Modi and his voters as well as within the party further augmenting Modi’s personal and intimate style of digitized politics (Sinha, 2017). The electoral success of the BJP, therefore, does not rely on its ideological project and Modi’s charisma alone, but the party’s cultivation of an ecosystem where an army of volunteers and paid professionals circulate content that feeds Hindu nationalist beliefs. As an ‘authoritarian innovation’, this network of actors plays a role in the erosion of democracy by ‘applying new technology’ (Curato and Fossati, 2020).

Building a subterranean network of WhatsApp groups, the BJP circulated WhatsApp messages with ‘stories’ to polarize the electorate; inciting feelings of pride and connection for some, and alienation and fear for others (Singh, 2019; Jaffrelot and Verniers, 2020; Williams et al, 2022). The content of

political messaging that circulated through BJP groups and beyond varied from those extolling Modi's greatness to anti-Muslim extreme speech. Special political groups were created by party members and volunteers on WhatsApp. Interestingly, among our respondents, relatively few people had subscribed to or been invited to political party groups, whereas almost all received political messages through family and friend groups. The former tended to encompass nuclear family groups with just immediate parents and offspring, siblings and cousins' groups and then 'extended family' groups with 10–30 members. Of the young adults we interviewed, their experiences of extended family WhatsApp groups were a spontaneous and animated topic for conversation: many narrated fights between cousins, the overwhelming volume of messages they received, the burden of expectation to react immediately to relatives' messages and their strategies for coping in this space by filtering, muting or exiting such groups (see [Williams et al, 2022](#)).

In 2014, the BJP created close to 10000 WhatsApp groups of party supporters. And with the BJP's IT cell having honed its strategy in the intervening state elections, by the 2019 national elections WhatsApp had become 'a major part of the party's arsenal' ([Singh, 2019](#), p 82). The BJP's IT cell created a network of 900,000 'cell phone pramukhs'. These grassroots volunteers and paid party workers used voter lists to map out the caste, religion and class background of the voters in their polling station to create WhatsApp 'interest groups' which were sent targeted messages generated by the BJP IT cell (Interview with BJP political consultant, April 2019). In some cases, the BJP also appropriated existing groups of entrepreneurs, where the admin or an active member of the group pledged support to the party ([Jaffrelot and Verniers, 2020](#)). Supporters of the party and Modi's bhakts (followers) were also encouraged, often through financial incentives, to send party-generated messages to their personal WhatsApp groups. Other BJP-linked groups which are not explicitly political are also part of the same ecosystem, for example a group in the hill town of Mandi in north India was formed to keep the town clean but the group admin was a BJP member ([Jaswal, 2024](#)). Later in the chapter we discuss neighbourhood groups which are formed for local governance but become spaces to bolster Hindu nationalist ideology. In these myriad ways, political messaging was rapidly disseminated across the networks of personal groups, originating from the BJP IT cell, but also other party proxies and sympathizers.

Subterranean networks ensured that mis/disinformation could spread without check. In 2018, BJP president Amit Shah declared to a large gathering of social media volunteers in the northern Indian state of Uttar Pradesh that the party had created 3.2 million WhatsApp groups in that one state alone and they can spread any message, whether 'true or false' ([McLaughlin, 2018](#)). He was confident that the party's 'WhatsApp warriors' were 'capable of delivering any message we want to the public'. And crucially,

he announced how the BJP could harness viral messages to ‘create a certain *mahaul* (a perception, atmosphere)’ among the electorate. Shah’s candid admission came around the time when his party’s government wanted WhatsApp and other ‘intermediaries’ to take liability for mob lynchings that had taken place due to misinformation about child kidnappings being spread through videos on WhatsApp (Banaji and Bhat, 2019). Despite WhatsApp being a key conduit of mis/disinformation (Chakrabarti, Stengel and Solanki, 2018), its popularity among political players in India tells us how WhatsApp’s unique selling points of privacy and encryption facilitate effective subterranean political propaganda.

The irony is that the same features of the app, such as end-to-end encryption which is promoted as a means to prevent state surveillance, also enables the politically powerful to infiltrate spaces of private communication among the electorate through a network of WhatsApp groups. As Subhash, a member of the BJP’s legal team, explained, the logic behind using WhatsApp concerned its affordability, scalability and the ability to piggyback on the ‘reputation of a network like family or friend groups, to spread a message’. After all, ‘[t]he consumer doesn’t know if it is fake or not because there is social proof of it, because it is sent by a relative’. The intimacy and trust that WhatsApp’s digital private spaces command for its users makes the spread of dis/misinformation possible.

The affective intensity of Hindu nationalism facilitated by WhatsApp’s subterranean storytelling infrastructure on WhatsApp produced uneven expression by design; where majoritarian truths prevailed and persisted as counter opinions became self-censored or silenced. Thus, in examining the appeal to emotion for politics in contemporary India, our research focused more on what it means for religious or political minorities to inhabit and negotiate intimate sociodigital spaces within the ‘global conjuncture of digitally enabled exclusionary politics’ (Udupa, Gagliardone and Hervik, 2021, p 12), and the implications for questions of voice and power, as well as feelings of belonging, identity, citizenship and political power in the context of Hindu nationalism in India.

In the case of Nitya’s extended family WhatsApp group discussed earlier in the chapter, the repetition of pro-Modi and anti-Muslim messaging within an intimate and trusted network reinforced their digital sociality and cemented ideological positions. They were intoxicated by the WhatsApp group as a new space for social interaction and enjoyed sharing political content that reaffirmed their world views. And, whether fake or not, their message gained legitimacy and truth by virtue of being forwarded by kin, people they trusted (Chakrabarti, Stengel and Solanki, 2018). Whereas, for Nitya, being in a group with her extended family members meant to routinely witness abusive rhetoric, imagery and ‘fake news’ designed to cultivate support for the BJP and Hindu nationalism more widely. More

importantly, her efforts to challenge the discriminatory overtones went unheard, where the potential to dissent from the majority view simply did not exist. Nitya then decided to leave the group.

The lived reality of WhatsApp challenges the company's techno-imaginary that digital private spaces are sites through which democratic practices are positively cultivated and where end-to-end encryption protects citizens from the surveillance of rogue states, criminals and hackers. Even as WhatsApp's digital private enclosures are spaces of security, intimacy and connection for some, we show later in the chapter, through the example of neighbourhood WhatsApp groups, that they are a place of fear, exclusion and lack of democratic engagement for others. How technology lands and how it is experienced is uneven. And so, intimate encrypted digital spaces produce contrasting terrains and experiences. If we take Nitya's group as an example, WhatsApp was a space for mis/disinformation for her which triggered emotions of anger, disappointment and exclusion. But for politically like-minded family members, the group was a space of sociodigital validation and connection. It is therefore important to consider how affective aspects of intimacies are differentially mediated by technology (Attwood, Hakim and Winch, 2017). Nitya's experiences are the production of the 'global intimate', with the intimate encompassing 'not only those entanglements rooted in the everyday, but also the subtlety of their interconnectedness to everyday intimacies in other places and times' (Mountz and Hyndman, 2006a, p 447). In this context global frictive intimacies concern not only the immediate political frictions between Nitya and her family members but also reflect and resonate with populist, nationalist and patriarchal politics and boundary marking more broadly.

Our research since the 2019 national election in India examined how those on the margins of Hindu nationalist politics navigate WhatsApp, how private spaces on WhatsApp become sites of exclusion and insecurity, how debate and dissent are not possible within these private spaces where hierarchies are reproduced, and digital-physical boundaries are made and remade. In this unevenness, people's experiences of lived democracy vary. A fragment of this research is discussed in the next section (see Williams et al, 2022; Kamra, Williams and Johar, 2023; Oza, Williams and Kamra, 2024). The privacy techtonics framework draws on a feminist geopolitical approach that examines the intersecting geopolitics of digital private spaces from the individual to the state and Big Tech. As Chapter 3 explained, digital private spaces or enclosures produced by Big Tech are increasingly central in political experience and democratic politics globally, and in India, the WhatsApp group occupies a crucial position in furthering the power of Hindu nationalism.

Affective appeals to Hindu nationalism often ride on the back of disinformation. In 2024, an online magazine called *Rest of the World* published

a piece tracing the journey of WhatsApp messages in a town called Mandi in the northern Indian state of Himachal Pradesh (Jaswal, 2024). One story narrated was about an electrician named K. Sharma. On 22 January 2024, when Prime Minister Narendra Modi inaugurated the Ram Mandir in Ayodhya, WhatsApp was abuzz with all kinds of messages. News channels covered every moment of the rituals. For supporters of Hindu nationalism, this was a significant moment. In 1992, groups of Hindu nationalist volunteers had demolished a Mughal era mosque called the Babri Masjid claiming that that was the birthplace of the Hindu god, Lord Ram. The site was a disputed site until 2019 when the Supreme Court gave permission for a new Ram temple to be built on the site (Singh, 2024). Modi inaugurated the temple in his capacity as the Prime Minister four months before the national elections and against principles of secularism enshrined in the Indian Constitution which stipulate that the state should be equi-distant from all religions. People posted celebratory messages on Facebook and in WhatsApp groups claiming it was Modi who brought Ram 'back', neighbourhoods organized rituals on the same day, and conversations alluded to how 'the Muslims' have been shown their rightful place.

In such a context, the report states that K. Sharma watched a video on Facebook where young Muslim men were being arrested in Mumbai for attacking a Hindu religious procession in support of the Ram Temple. He shared the video on his neighbourhood WhatsApp group, and from there the video reached 1700 Mandi residents via several WhatsApp groups. However, it turned out that this was an old video from a 2022 protest in Hyderabad, miles away from Mandi. Misinformation had spread in Mandi and could have even led to violence against the Muslim residents there by Hindus who were enthused about the temple inauguration. No one can say with certainty that a party member or volunteer created the video, neither can one identify who sent it first. But deeper research by the magazine into the WhatsApp groups of Mandi revealed that the BJP was involved (Jaswal, 2024). The chain of messaging from the IT cell to cell phone pramukhs to ordinary citizens and within citizens is not always possible to trace but that is how targeted political messaging travels, alongside misinformation and disinformation. In this way, the digital private spaces of WhatsApp become sites of propaganda and Hindu nationalist politics in India.

The BJP may have been the first mover and the party that creates and circulates the most volume of WhatsApp content, but all political parties, big and small, have now stepped into the fray. Parties generate and coordinate the circulation of content for different social media platforms, so there would be a special group of people appointed for creating messages, memes and videos meant for WhatsApp circulation. Parties then use WhatsApp groups and broadcast lists to send out the content. The Aam Aadmi Party (AAP) in Delhi, for example, also uses WhatsApp for political communication. Mir,

a university student who was a member of AAP's student wing and worked with AAP's social media team, told our team member that they focus more on WhatsApp because people tend to trust what they receive on the medium, as compared to say, Facebook and Instagram.

Another AAP politician, in an interview to [Narayan and Narayanan \(2024, p 99\)](#) pointed out that messages for WhatsApp have to be 'curated' very differently from those meant for Twitter and Facebook. He adds that they tend to use more emojis in WhatsApp messages and can create longer text messages. Mir had further explained to us how the party strategy was to have different social media teams for each constituency. A team of 5–6 people would take care of different social media platforms among themselves to reach out to as many people as possible within the geographical area assigned to them. They would target existing WhatsApp groups and create some new ones and use broadcast lists to send messages about AAP's work, policies and the candidate contesting from the area. 'You can only forward messages to five people at a time on WhatsApp and that is why we use groups and broadcast lists to reach out to more people'. In 2018, when WhatsApp had limited the number of people you can forward a message to five, other features of the app such as groups and broadcast lists became more popular with politicians to reach out to a larger number of people.

During the COVID-19 pandemic, parties began to rely much more on digital media for reaching out to voters during elections. Smaller political parties across the country would also use WhatsApp with their limited resources. As Kiran Kumar, a coordinator for the Vikassheel Insaan Party in the eastern Indian state of Bihar pointed out, 'I created 2–4 groups to send information to people in my area and I am the admin of all these groups. We use WhatsApp because it is a secure platform, it is end-to-end encrypted'. We spoke to him during the campaign period for the 2020 Bihar state election, when due to COVID-19, much of the campaigning had moved online and smaller parties also felt the need to draw on digital technology much more than usual. A local worker of the Lok Janshakti Party (LJP), Shyam Paswan, also told us in an interview for the project that social media teams of parties are more important now and detailed his role as one who sends the messages which the LJP team relays to him. Parties organize their WhatsApp groups and networks in different ways based on the resources they have. Personal networks are a defining feature of WhatsApp and political parties capitalize on that to amplify their messaging and target more people.

WhatsApp's increased salience in political messaging, however, goes alongside a continued preference among parties and voters for in-person campaigning. In modern Indian political campaigns, parties use 'a two-way content-complementarity' – where they are using both digital and in-person campaigning ([Sheikh, 2024](#)). Digital messaging serves a dual role for political parties: (1) keeping voters informed about in-person campaigns during

elections (dates and circulating videos after an event), and (2) spreading messages with political content and propaganda at all times, in the periods between elections. Among existing digital messaging apps, it is WhatsApp that is most used by political parties for their preferred political narratives to keep circulating during elections and at other times. Ordinary citizens became a part of the process when they forward messages and participate in political talk on WhatsApp in their everyday lives.

WhatsApp in the neighbourhood

Banaji and Bhat (2022) argue that we know less about the affective implications of Hindu nationalism's dominance in the digital-political lives of political and religious minorities, on whose bodies the boundaries of Hindu nation are reinscribed. Taking a cue from them, we examine the experiences of people living in the shadows of Hindu nationalism to elucidate how sociopolitical subjectivities and everyday experiences are shaped within a right-wing digital ecosystem rooted in anti-Muslim, if not anti-minority, prejudice. We ask: what does it mean for religious or political minorities to inhabit and negotiate intimate sociodigital spaces within this context? What are the implications for questions of voice and power, as well as feelings of belonging, identity and citizenship and how are civic and political relationships being transformed? We show next how religious minorities and lower-class workers are excluded and policed through WhatsApp's private digital spaces in middle-class urban neighbourhoods of New Delhi.

In the everyday life of Indian citizens, private digital spaces often mirror the nation's politics and social divides. Neighbourhood WhatsApp groups, for instance, provide a glimpse into the everyday politics of private digital spaces. Our research revealed how WhatsApp's private spaces have become significant for residents in neighbourhoods and apartment complexes to connect with each other on shared issues and carry out governance of their locality. Hate speech, misinformation and Hindu right-wing messages widely circulated in groups people shared with neighbours in the middle-class and upper-middle-class neighbourhoods of New Delhi. Neighbourhood WhatsApp groups comprise two kinds: official groups created and run by the Resident Welfare Associations (RWAs) and other groups that residents of a neighbourhood form unofficially. Formed to connect residents with each other, neighbourhood WhatsApp groups are also private digital spaces where members clashed on political lines and forwarded messages that made minority communities feel threatened. RWA leaders also used WhatsApp for surveillance, to police lower classes and members of minoritized groups, in this way, WhatsApp groups were sites of grassroots authoritarianism within India's larger political context (Kamra, Williams and Johar, 2023; Oza, Williams and Kamra, 2024).

This section explores how neighbourhood WhatsApp groups contribute towards the making of an authoritarian right-wing Hindu nationalist state. It draws on research done in 2019 and 2020 which focused on middle-class neighbourhoods of New Delhi where neighbours connected with each other through WhatsApp.

RWAs are voluntary grassroots organizations that typically represent the interests of India's urban middle classes living in gated complexes and apartment blocks. Their formation is supported by local municipal councils, which expect RWAs to act as their intermediary with citizens of a locality. RWA groups perform the connecting function with a clear chain of command where the RWA president is the group admin and often directs and controls the messaging. RWAs are voluntary grassroots organizations that typically represent the interests of India's urban middle classes living in gated complexes and apartment blocks. Association members are elected or nominated to fulfil primary duties on behalf of local residents concerning the maintenance of roads, sanitation and ensuring the safety of the neighbourhood. While RWAs operate on a pro bono basis they are governed by constitutional rules which, in theory, keep their powers in check. In Delhi, RWAs have existed since the 1970s. They received official status in 2000 through the Bhagidari (partnership) scheme introduced by the then Congress-led Delhi government. The initiative aimed to forge a closer relationship between the government and citizens by giving powers to local neighbourhood organizations. However, the expectation that encouraging middle-class civic participation in urban areas and strengthening citizen–state relations would deepen democracy has been roundly contested.

The urban middle classes have succeeded in making the city in their image at the exclusion of class, caste and racial outsiders (Harriss, 2006; Bhan, 2016). The 'participation' of the middle classes through such associations has played a role in increasing political inequality in the city by excluding the informal working class (Harriss, 2006). There is a visible contradiction between the retreat of middle classes into gated urban enclosures, with physical boundaries and security personnel on the one hand and the apparent deepening of 'democratic sentiment' and so-called local governance taking place within these spaces on the other hand (Srivastava, 2015). So, while RWAs may perform democratic practices such as holding yearly elections and promoting inclusion through 'women's wings', in practice they are composed of largely male, 'elderly, retired from the armed forces' representatives (Srivastava, 2015, p 89). They also fail to incorporate any schemes for the urban poor making RWAs far from inclusionary and democratic (Tawa Lama-Rewal, 2007). Participation and empowerment through the decentralization of power to RWAs paradoxically reinforced middle- and upper-class interests and these groups tend to be less critical of the government.

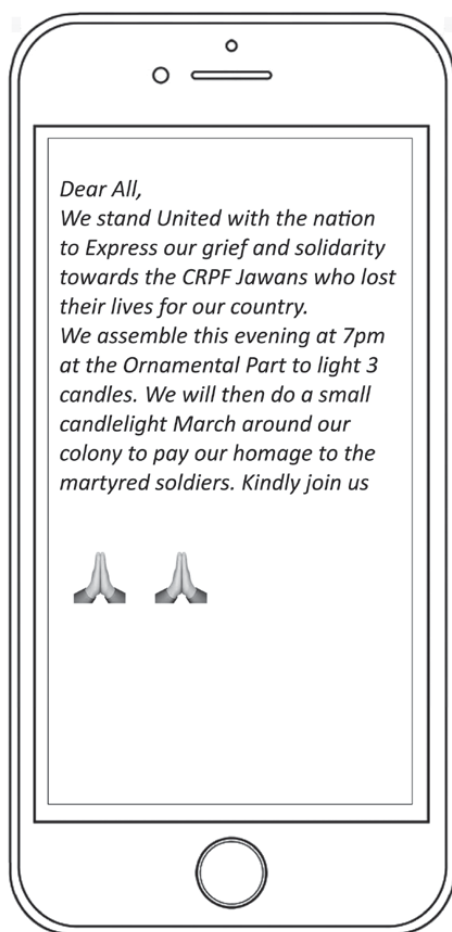
Participants remarked on how the private digital space was being fashioned in a particular image and engendered a pro-Modi, and often pro-Hindu nationalist agenda. Minority religious residents drew attention to the BJP orientated images that their RWA group admins used as their group's status or 'Display Picture'. For example, during interviews in 2019, several Muslim and Christian respondents told us that they found the choice of the lotus flower (the party symbol of the BJP, regarded as sacred in Hinduism) or Narendra Modi as the group profile image, sent a subtle yet mundane signal to the group that demarcated the boundaries of politico-religious membership. It was therefore assumed that everyone on the group subscribed to Modi and the BJP's Hindu nationalist agenda, which left some residents feeling sidelined, and denied the space to voice their religious and political allegiances within the digital socio-spatial neighbourhood.

This tension surfaced, for example, in the aftermath of the Pulwama attacks in February 2019 when the content circulated on RWA WhatsApp groups sought to vilify Pakistani aggressors, and by association, India's Muslims. All those not publicly and visibly in support of Modi's retaliatory violence were presumed, if not pronounced to be 'anti national' (Sinha, 2017). The posts on the WhatsApp group were entangled with events organized in the neighbourhood to honour deceased soldiers and, at which, congregations were heard shouting anti-Pakistan slogans. Within New Delhi's middle-class neighbourhoods, it became very common to see events with flag-hoisting and patriotic Bollywood songs blaring out from large speakers. Communication about such events was circulated on neighbourhood WhatsApp groups, often by RWA presidents themselves (see Figure 4.1). The event, meant to be one where deceased soldiers were to be honoured, also became a space where anti-Pakistan slogans were conflated with anti-Muslim ones and Muslim residents of the locality felt a sense of fear. The neighbourhood, enabled by its WhatsApp spaces, played a role in empowering Hindu right opinion and underpinning more public offline utterances of intolerance.

Expressions of support for Hindu nationalism in the digital-physical spaces of the neighbourhood worked to induce fear and anxiety among those who did not support the project. They were affected by the repetition of nationalist and anti-minority content within the neighbourhood WhatsApp groups. The subterranean storytelling infrastructure, through messages inciting fear, hatred and anxiety, created and reinforced boundaries among residents. Despite feeling threatened and marginalized, it was difficult for residents to leave the neighbourhood groups as they relied on updates sent to the groups to get information about everyday logistics such as the timing of power cuts and water supply.

But staying updated also meant facing attacks. Sadiq was a middle-class Muslim in his early fifties who worked as a volunteer for the Aam Admi

Figure 4.1: WhatsApp message to the Residents Welfare Association WhatsApp group, 15 February 2019



Party. In conversation with a member of our project, he condemned hate speech and as ‘Pulwama’ inevitably entered their conversation, he lowered his voice and said: ‘I’ll share an experience with you, Mr. Jain lives in the same colony as I do. He forwarded a message about the Pulwama attack to me and on our neighbourhood group. It was about Muslims’. Sadiq decided to question his neighbour face to face. He narrated: ‘I went up to him and asked, why have you forwarded this to me? Do you even know where this message has originated?’ In front of everyone he replied, ‘You will say such a thing. You should go to Pakistan ... He was my good friend. I am scared now. You cannot speak your mind with anyone. I’m a minority, I’m worried. It’s best to stay within ourselves now.’ Sadiq not only felt excluded but also

attacked. He was emotionally affected by the exchange and the fact that such messages would continue on the neighbourhood groups. Mr. Jain was repeating the rhetoric of some Hindu nationalists who think that Muslims belong to Pakistan rather than India. Sadiq felt like a ‘digital denizen’ who was excluded from normalizing narratives and practices that reproduce the hegemony of Hindu nationalism in digital spaces (Oza, Williams and Kamra, 2024). Experiences like Sadiq’s were faced by many who would try to challenge the dominant Hindu-right-wing narratives on neighbourhood groups, but especially if they belonged to religious minority groups.

Anti-minority content in the COVID-19 pandemic

Anti-minority content particularly thrived during the COVID-19 lockdowns too, when Muslims were scapegoated for spreading the coronavirus in India. Memes, messages and movies constructed a spectre of internal threats posed by Muslims. In the early days of the lockdown, the epicentre of India’s coronavirus outbreak was widely attributed to a Tablighi Jamaat Congress in Nizamuddin, New Delhi, and from where visiting Muslims travelled back to their homes across India. In India’s official lists of COVID-positive cases, the Tablighi Jamaat cases appeared as a separate category, whereas other cases were classified according to region rather than venue. This racial construct singled out and portrayed Muslims as prime vectors for viral transmission. In a paradoxical act, images depicting the persistence of large Hindu religious gatherings were circulated to demonstrate the strength and bravery of India’s Hindu devotees in the face of the virus. The threat of the diseased Muslim body was also located closer to home, within the neighbourhood.

We also observed a variety of forwarded messages that framed local Muslim store owners and vegetable vendors as carriers of COVID-19. The content simultaneously pathologized Muslim bodies, induced fear of the ‘other’ and created an ethic of care towards majority Hindus on the WhatsApp groups by warning them of the threat and protecting group members from the virus. Even as many of these video clips and messages were later denounced as fake, that did not stop the everyday vilification of Muslims and some localities even banning Muslim vegetable vendors from entering inside the gates.

Moreover, videos continued to be forwarded on the ‘Manor Park’ RWA group (one group we followed during our research) by residents adding authority to the narrative of the ‘Muslim threat’. A talking heads film titled ‘BJP against Islam in India’ presented by the YouTube presenter D. K. Dubey explained how the BJP’s actions against Muslims were ‘good’ for India and Indians. The hyperbolic presentation contended that the Tablighi Jamaat spread COVID-19 as part of a larger policy hatched by Muslims to ‘take over’ India in different ways, from increasing the Muslim demographic to waging Islamist terrorism.

This discourse is part of the right-wing propaganda that perceives India's Muslims as a threat to the purity of the Hindu nation (Appadurai, 2006) and exploits fear and anger to justify their physical and rhetorical 'othering' (Jaffrelot, 2021). The circulation and consumption of such a video in the aftermath of the 'Tablighi Jamaat-incident' on WhatsApp served to reiterate and amplify assiduous imaginaries of the 'dangerous Muslim' via people's smartphones.

Care and disciplining

The pandemic induced a shift from everyday encounters on neighbourhood streets and living rooms to the digital private spaces of WhatsApp group chats. In such a context, the neighbourhood group became a space of exclusionary care and belonging. The WhatsApp group has arguably engendered a sense of belonging and 'affective mooring' for its Hindu majority members (Dixon, 2017, p 501). Drawing on research of a WhatsApp group in Johannesburg, South Africa, Dixon (2017) shows how WhatsApp is central to producing a shared idea of the neighbourhood as people can affirm feelings of fear, paranoia and/or safety within this digital private space. Dixon highlights the paradoxical tensions present in the production of neighbourliness and social cohesion which entangles information sharing and the caring ideals of protection underpinned by everyday surveillance and control (Dixon, 2017). These contradictory sentiments were also visible in the wake of India's March 2020 lockdown as RWA WhatsApp group communication became dominated by the concerns of disease transmission and containment as well as neighbourly gestures of support and care.

However, the gestures of care did not extend to all residents. Working-class personnel were portrayed as presenting the most immediate and intimate 'threat' from COVID-19, given the mobile nature of their work and dense living conditions in lower-income settlements. During the first lockdown, domestic workers were forbidden, and subsequently often laid off from servicing homes. Yet, even after nationwide restrictions on access to homes were eased, RWAs continued to exercise their autonomy on this matter, with some neighbourhoods continuing to ban the entry of domestic workers. This debate animated the national media, dominated as it is by middle-class and elite opinion as well as WhatsApp group exchanges that we observed. For instance, domestic helpers were banned by RWAs from using communal lifts and instead forced to climb the stairs even in multistorey buildings, to 'protect' local residents. The treatment of lower-class service workers by RWAs exposed the deep-seated anxieties about the service classes and a middle-class obsession with policing the behaviour of lower classes. Making rules about whether to allow domestic workers or not were often broadcast on neighbourhood WhatsApp groups and discussion, with no consideration for the classist nature of this discourse.

The contradictions were most visible when alongside the rhetoric of protection for all; there was a simultaneous production of the Muslim as the villain who needs to be excluded, not protected. The production of fear through the construct of the Muslim ‘other’ as a site of suspicion, threat and disease is not new in India but rather builds upon a history of physical and ‘routine violence’ articulated by the Hindu right against India’s largest religious minority (Pandey, 2005). And during the COVID-19 lockdowns and afterwards, this routine violence represented a leitmotif of the government’s shift towards authoritarian rule. The link between authoritarianism and ethnocentrism has been well documented (Adorno, 2019). Yet, the demonizing of diseased ‘others’ takes on new resonance in the pandemic which witnessed ‘an increase in nationalistic rhetoric to promote both the acceptance of legitimate measures designed to prevent the spread of disease and authoritarian policies disguised as such’ (Hartman et al, 2021).

WhatsApp facilitated the exchange of pathologized racial and class content on WhatsApp groups – consumed alongside other social media and daily activities – normalized and reinforced local boundaries (Kamra and Khatri, 2021). These drew clear distinctions between racial and class threats versus Indian citizens/residents who should be protected and secured against the virus. The daily stream of WhatsApp content on RWA groups therefore fuelled an atmosphere of fear and threat that justified the assertion of grassroots authoritarian practices to secure the neighbourhood, but that inescapably impinged on individual freedoms and privacy. This inevitably involved the surveillance of all bodies in the neighbourhood, though to differing degrees.

WhatsApp for surveillance

Everyday politics of hate and authoritarianism in the neighbourhood also went hand in hand with everyday surveillance and the erosion of individual and collective privacy. We typically think of surveillance as a ‘specialised activity’ conducted by specialist agencies, but domestic or neighbourhood surveillance is an everyday feature of geographically proximal communities (Lyon, 2018, p 6). For instance, the figure of the ‘curtain twitcher’ who keeps a close eye on neighbourhood activities would be a familiar one to Euro-American audiences. For young women in India – whose bodies are intertwined with notions of family honour – community-level surveillance has long been a pervasive part of everyday life (Butalia, 1993). But the ubiquity of digital technologies means that ‘watching has become a way of life’ (Lyon, 2018, p 4) with increased technological and non-technological opportunities for ‘focused, systematic and routine attention to personal details for purposes of influence, management, protection or direction’

(Lyon, 2018, p 14; see also Monahan, 2017). The networked privacy and immediacy of the RWA WhatsApp group facilitated more intrusive and omniscient practices of neighbourhood surveillance that were intended to influence behaviour and protect the locality from COVID-19.

Our research demonstrates how in the context of COVID-19 and wider authoritarian cultures, surveillance techniques targeted and constructed a hierarchy of outsiders, as well as contagious insiders or those who transgressed the rules and represented irresponsible 'others'. As Monahan has argued, '[t]hrough the imposition of categories, processes, and differential forms of exposure, surveillance becomes a project of social ordering and world-making, even if its efficacy ... is limited or inconsistent' (Monahan, 2017, p 192). The surveillance of residents by other residents was a ubiquitous practice across RWAs. Grassroots surveillance was not only aimed at controlling the behaviour and mobility of alien 'outsiders' but also concerned the policing of middle-class bodies internally as well. For example, on 31 March 2020, just a week into India's national lockdown, a message was shared on a WhatsApp group in a middle-class Delhi neighbourhood called the 'Manor Park' RWA group which read that 'meeting a friend in the locality is also an irresponsible act these days'. The sender personally captioned the message with the words: 'I am sharing this because some people in the building are involved in such activities'. Similarly, photos were taken of residents apparently leaving their apartment complex during lockdown without their permission. And in another RWA group, on 12 April 2020, a resident posted pictures of neighbours leaving their flat for a walk, suffixing the images with a warning that this behaviour was 'breaking the codes of lockdown'. Since walks were not prohibited during that period, the resident's condemnation was overzealous. The ubiquity of micro-level surveillance therefore undermined individual privacy and served to stigmatize diseased bodies and transgressive behaviour through the effect of the WhatsApp panopticon. Ironically, the private space of the WhatsApp group becomes a means for citizens to lose privacy, where private groups are used to make things 'public'.

The hate speech, surveillance and exclusionary tactics of neighbourhood WhatsApp groups created spaces of grassroots authoritarianism (Kamra, Williams and Johar, 2023). However, authoritarianism and hate were sometimes challenged on neighbourhood WhatsApp groups. Fractures in state and grassroots authority were visible through the circulation of counternarratives that questioned the validity of pro-Hindu nationalist digital content and challenged the authority of RWA office bearers. For example, although anti-Muslim content was fairly ubiquitous on RWA WhatsApp groups, there were attempts to question the validity of information that constructed India's Muslims as vectors of contagion. In

one such forwarded message, the original author writes about his father's experiences in Nagpur, western India, but the message also resonated within New Delhi neighbourhoods where similar narratives about diseased bodies were being circulated:

My parents have been buying groceries from a supermarket owned by a Malayali Muslim for many many years. The shop is nearby house and trustworthy. Yesterday my father received a WhatsApp forward asking him not to go to the shop as the owner was infested with corona virus and the goods in the shop were infected too. My father [sic] didn't fall for the propaganda and called the person the forward asked him the source of the forward. The person who sent the forward had received it from someone else. My dad then called DC [the Police District Commissioner] office and complained about the fake news. DC office also confirmed that the news was fake. I don't know if corona virus will impact the 'Indian' society but communal virus ... will irreversibly damage the society. I feel helpless and depressed. (message on a group named 'WA Hotspot', 9 April 2020)

Those forwarding the text were attempting to disrupt the prevailing dominant popular imaginaries of Muslims as contagious, dangerous others, and reimagine the socio-spatial city as one that is not divided along communal lines. Though as the original author concludes, the potential for this in the context of Hindutva and COVID-19 is uncertain, if not unlikely. It is important to note that such interventions were really quite rare on the WhatsApp groups we came to know about.

From the neighbourhood to the nation, WhatsApp *is* political infrastructure. The private and networked nature of WhatsApp's infrastructure has inspired (party) political organizations and become the site for everyday 'political talk'. And, as we argue in the final section, WhatsApp is now increasingly playing a role in delivering the Indian government's digital public infrastructure.

Digital public-private infrastructures

The 'Digital India' initiative was one of Narendra Modi's flagship policies when he was first elected as Prime Minister in 2014 and continues to drive a digital and AI transformation in Indian society and economy today. Narendra Modi is regarded as the 'first national leader whose political fortunes were realized in large part due to the country's adoption of digital technologies', where others have met resistance (Sukumar, 2019, p 186). Modi urged his compatriots to viscerally embrace digital technology. The BJP's manifesto for the 2014 General Elections stressed the 'maximum application of technology'

to ‘all aspects of governance’ (Sukumar, 2019, 185–186). As a key pillar of Modi’s first term in office, ‘Digital India’ was intended ‘to transform India into a digitally empowered society and knowledge economy’ (Ministry of Electronics and Information Technology, 2019). It was underpinned by the utopian visions of international development organizations and digital gurus who prophesied that a digital ‘reboot’ would fix India’s development and democratic challenges (Nilekani and Shah, 2016). Such visions are not unique to Indian modernity. In Kenya, techno-utopian narratives were strategically mobilized by developers and state actors to craft visions of nationhood (Poggiali, 2017). Yet, digital techno narratives only go so far in achieving the promised utopias and often exacerbate or create new cleavages in already unequal societies (see Datta, 2018).

Modi’s strategy of state-led digitization has relied on the government’s close partnership with technocrats, Fintechs, software and telecoms companies and progressively established the India Stack ecosystem (see Dattani, 2019). Understood as India’s digital public infrastructure (DPI), the India Stack has multiple layers: (1) the biometric database Aadhaar is its foundational identity or presence-less layer; (2) a paperless layer replaces physical documents with electronic transactions and records enabled through services like eSign and DigiLocker; (3) a cashless layer fulfilled through the Unified Payments Interface (UPI) allows for immediate digital transactions between parties and is likened to digital payment rails; and (4) a consent layer which consists of an electronic management system called DEPA to facilitate the sharing of user data between platforms and parties (Parsheera, 2024).

Often celebrated as a model for digital delivery globally, DPI has become a key diplomacy tool for Modi. During his G20 Presidency in 2023, Modi used DPI to position India as a voice of the global south and established an important global consensus on DPI as a set of shared secure and interoperable digital systems to provide equitable access to public and private services at scale (Chaudhuri, 2023).

India’s DPI relies on private partners and platforms to help citizens and businesses interact with the stack’s layers and services. In recent years, the government has actively promoted WhatsApp’s private digital infrastructure to facilitate the delivery of its digital public infrastructure at scale. Take for example, an announcement by the Delhi government in August 2025 of its intentions to set up a WhatsApp-based application system for driving licences and marriage certificates (Livemint, 2025). This announcement followed the launch of WhatsApp chatbots in the states of Tamil Nadu and Andhra Pradesh to consolidate public services under a single phone number (Rohit, 2025; TimesofIndia.com, 2025). The chatbots help people with paying for utilities, booking bus tickets, filing for grievance redressal and paying municipal taxes. For Meta, partnering with regional governments on such initiatives raises their profile as a private company committed to delivering

public goods while Indian officials can announce their success in making public services more convenient and accessible to citizens. WhatsApp India has also revealed its plans to use Meta's Llama AI to power digital governance in the future (Rohit, 2025). The deepening relationship between Meta/WhatsApp and the adoption of AI in the delivery of India's digital public infrastructure raises inherent tensions around the 'publicness' of DPI. Critics warn of the risk that India is 'anchoring critical citizen interactions to a platform if doesn't control' (Shaikh, 2025). Afterall, Meta is a private company delivering a public service while privately profiting from its collection and processing of Indian users' behavioural and metadata.

Politicians continue to capitalize on WhatsApp in new ways for political communication and to connect with citizens and party members. In September 2023, Narendra Modi announced his own WhatsApp channel for connecting directly with his 'followers'. While Modi regularly posts on X (formerly Twitter), Facebook and Instagram, joining a WhatsApp channel signalled how he wants to capitalize on different features of an app which ensures more intimate connections, even when it is through a 'public' channel. The first message that Modi sent out on his WhatsApp channel said, 'Thrilled to join the WhatsApp community! It is yet another step closer in our journey of continued interactions. Let's stay connected here!' In the run-up to the 2024 elections, Modi used WhatsApp Business to mass message citizens, which become a controversy as Meta does not allow political parties to use WhatsApp Business. We discuss this in [Chapter 8](#). The entanglement of Big Tech and government power is central to the mobilization of private digital spaces for politics.

It is important to juxtapose the Indian government's drive for state-led digitization and its own use of digital technologies for political communication alongside its public mistrust of Big Tech and Indian citizens' use of social media to challenge its political authority. Within this context the Indian state exercises 'architectures of control' to determine what citizens can say and do, or not, through the internet (Isin and Ruppert, 2020, p 97). For example, the government's amendments to the IT rules in India 2021 imposed an obligation on social media companies to abide by local laws and constitutional rights of Indian users (Ministry of Electronics and Information Technology, 2021). In practice this means the Indian government has authority to decide on the suitability of posts, with Facebook and Twitter being reprimanded for not removing information deemed to be 'anti-national'. Meanwhile, the government issues internet shutdowns to limit its citizens' digital communications. According to the Software Freedom Law Centre, since 2012 there have been 665 such cases ordered in India (Sharma, 2022). The government justifies internet shutdowns based on national security threats arising from misinformation and rumours circulating in social media, that curbing the flow of information is

important for maintaining law and order and peaceful community relations. The shutdown of internet infrastructure represents a material censorship of communication and information flows disproportionately targeted to further marginalize India's regional, religious and political minorities (AP, 2020). Such tendencies towards digital closures severely challenge India's global diplomacy in advocating for digital public infrastructure.

Conclusion

Digital private spaces have implications for democracy globally. They encourage greater participation and connection between citizens and political leaders and increasingly facilitate digital governance. But digital technologies and spaces are saturated by and produced through political relations. In our research in India, the sociopolitical differences of class, religion and gender came to the fore in how WhatsApp is exploited by political parties as well as how citizens engaged in everyday politics. The case of Nitya's family group illustrates how WhatsApp enables the production and reproduction of intimate boundaries and belonging that strengthened Hindu nationalist sentiment. Such boundary-making practices function to include but also exclude, particularly those deemed outside the 'mainstream' and belonging to minority religious groups and lower classes. Nitya, like others negotiated frictions at these boundaries by silencing, muting and exiting WhatsApp's sociodigital spaces.

The mobilization of WhatsApp's subterranean storytelling infrastructure for right-wing politics across the world undermines WhatsApp's vision and commitment to a private future that facilitates democratic practices for all. On the one hand the BJP's form of authoritarian populist politics has been and is being intentionally augmented through WhatsApp's encrypted digital messaging. And on the other hand, WhatsApp's maturing business has benefited from the 'weaponization' of its product by the BJP and its supporters, both in campaign mode and in power. Read in this way, WhatsApp and India's Hindu nationalist fortunes are positively entangled with everyday life in India. This relationship is becoming further entrenched by the government's embrace of WhatsApp as a private company to deliver aspects of India's digital public infrastructure. The rise in AI content in digital private messaging and AI agents in digital governance will only complicate the intimate geopolitics of WhatsApp and everyday experiences of its digital private spaces. In the [next chapter](#) we further examine the role of WhatsApp as a private authority in India and how 'privacy' is used to reproduce WhatsApp's power within geolegal and geopolitical spaces.

Privacy and the Law

The fundamental right to privacy might be universally recognized, pronounced in all of the major international and regional human rights documents (UN, 1948, pp 116–117). Yet, how privacy is legally articulated and regulated varies between geographical and institutional contexts. The introduction of GDPR in Europe in 2018, the shift towards more privacy focused laws in the USA and the declaration of privacy as a fundamental right in the Indian Supreme Court all infer that privacy is being taken more seriously than ever by law makers and civil society (Matthan, 2018). In practice, corporations are required to self-regulate, which has created a scenario in which tech companies push the boundaries of what is legally viable given their dependence on data for ‘surveillance capitalism’ (Zuboff, 2019). This has normalized games of cat and mouse between corporations and the regulators belatedly levying fines and penalties only after tech companies have overreached. Meta’s (previously Facebook’s) 10-Q reports which detail a company’s financial position, operations and legal proceedings over each quarter for US authorities, routinely cite privacy laws and pending lawsuits in different territories as potential risks to their company’s innovation and growth (Zuboff, 2019, pp 103–106).

For Shoshana Zuboff, the rise of ‘surveillance capitalism’ is the product of ‘a kind of lawlessness’ produced in part through Big Tech’s intent on blocking, resisting and weakening any kind of regulation and legislation that presents an ‘existential threat[s] to the frictionless flow of behavioural surplus’ (2019, pp 104–105). Legal scholar, Julie Cohen counters Zuboff’s characterization of this assertion ‘of a right to lawless space’ (Cohen, 2019a) by inserting a more rarefied approach to the law and legality that does not mistake Big Tech’s ‘lawlessness’ for the law’s absence, but instead interrogates *how* Big Tech resists, appropriates, innovates and narrates legal tools and institutions to further their own interests and in ways which shift and embed legal and economic norms (Cohen, 2019a, p 241). Like Cohen and legal geography scholarship we approach law and legality as productive of not

only the economy but also space and time (Braverman et al, 2014; Delaney, 2015; Jeffrey, 2019).

So, it is not just what the law and legal materials say or do not say that is important for realizing privacy, but how the law is interpreted and implemented within a geopolitical context that is most interesting. That is, we are concerned with the social life of privacy laws, regulations and associated policies. Waldman (2021) argues that within a context of self-regulation, the information industry can mobilize privacy laws to achieve their profit-making goals. In the US, voluntary disclosures about data practice are the foundation of the federal ‘notice and consent’ approach to internet privacy. Meanwhile the EU’s GDPR is more prescriptive about the substance of privacy policies. In India, the Digital Personal Data Protection Act, 2023 (DPDPA) was recently enacted and the draft rules published at the end of 2024 meaning that while the principle of privacy as a fundamental right has been established it is only just being codified in terms of digital and data rights. Privacy policies discursively construct privacy to demonstrate compliance with the relevant privacy laws and frameworks; in the absence of local jurisdictional data privacy regulation privacy is read through the company’s jurisdiction.

As a form of socio-legal contract between citizens and Big Tech, the logic is that technology companies post privacy policies which users are expected to read and understand the meaning and implications of and then follow rational decision-making processes to engage with the companies which they believe provide an acceptable level of privacy. In practice, privacy policies take too long to read and are written in an opaque and often ambiguous style that makes them difficult to understand (Reidenberg et al, 2015). The result is that few users have the time or inclination to closely and carefully engage with privacy policies, or framed another way, for users to actively protect their privacy rights there is a time cost imposed on individuals to even begin to make informed decisions about their data (McDonald and Cranor, 2008).

Legal material can also play a role in shifting socio-legal norms (Reed and Murray, 2018). The privacy policies of technology companies articulate narratives or stories about data which normalizes our ways of thinking about our data and our privacy. For instance, they tell us that user data is an essential commodity required by technology companies to develop their product or that product or policy innovations are inevitable for progress (Véliz, 2021, pp 70–71). They may also conceal the ‘banal, structural data leak which is built into the design of the apps’ (Shipp, 2022, p 254). The privacy policies and the privacy narratives of global technology products such as WhatsApp, play a role in shaping and gradually shifting local and global privacy norms.

While privacy policies may *appear* to be aimed at individual users, they are written primarily with the company’s interests in mind and for an

imagined audience of (privacy) lawyers and government officials. As public documents, privacy policies and associated statements give shape to and confirm technology companies' legitimacy as a public good. The substance and socialization of privacy policies, how they dialogue with state governance and legal jurisdictions, provide insight into how Meta (and WhatsApp) seeks to produce, if not, reproduce, itself as a legitimate private authority within geopolitical spaces (S. [Srivastava, 2023](#)). [Waldman \(2021\)](#) argues that tech corporations have successfully dominated privacy narratives concerning our data: influencing how we think about privacy in a way that entrenches corporate-friendly ideas as common sense and furthers corporate interests over others ([Waldman 2021](#), p 6). So, while it may look like tech companies are following the law, in reality they are 'reframing it to achieve their own data-extractive ends' ([Waldman, 2021](#), p 7). Yet, given the uneven power of privacy policies and regulatory environments, governments have increasingly turned to antitrust and competition law to respond to privacy issues ([Pasquale, 2013](#); [Carugati, 2023](#)).

We conceive of the privacy policy as more than a legal device for WhatsApp to protect its corporate interests. As a material document it comes to life through its articulation to establish WhatsApp's legitimacy within jurisdictions, and we also show how it becomes a site for citizens and the state to contest WhatsApp's entrepreneurial private authority. Given that 'the status of Big Tech as a private authority means that there must be consent of the governed for it to be legitimate' ([Srivastava 2023](#), p 993) and, moreover, of the state too. This chapter turns attention to the social life of WhatsApp's privacy policies and examines the geopolitical and legal debates within which its privacy policies are updated, received, interpreted and contested. We want to understand how WhatsApp constructs its shifting and contingent privacy realities in dialogue with its ambitions for growth, its technical infrastructures, individual politics and ethics, user-citizens and the government of India.

Part of the power of Big Tech lies in the narratives it tells itself and us about data and about our privacy and where privacy is power, feminist scholars have argued 'privacy has long been used as a pretext to protect traditional hierarchies of power' ([Waldman, 2021](#), p 12; [Gajda, 2022](#); [Menon, 2022](#)). To understand how privacy is used to reproduce WhatsApp's power within geolegal and geopolitical spaces this chapter draws on analysis of WhatsApp's privacy policies, Meta's 10-Q submissions, read-outs from Meta's quarterly earnings calls, regulator communications and legal proceedings in India, public interviews with Meta's leaders as well as of the interviews we conducted with litigants, civil society organizations and technology journalists in India. The chapter unfolds through the following five sections. First, we situate WhatsApp's privacy policies and their 'un-making of privacy' within the geopolitical economy; second, we

examine how different actors contested the new contours of WhatsApp's privacy policy within and beyond India's courts before analysing the key themes that emerged through these contestations. Third, in questioning consent, choice and control we interrogate the apparent fiction of 'consent' through which WhatsApp defines its relationship with citizen-users. The fourth section perceives the geolegalities of digital privacy regulations to focus on private corporate power, data and national sovereignty and legal jurisdictions which characterized the uneven and shifting landscapes of power between WhatsApp and the Government of India. The final section argues that the struggle over the meaning of privacy is also a competition over trust and authority between WhatsApp and the Indian government, and its user-citizens.

WhatsApp's privacy policy in context: un-making privacy, as progress

In the geolegal context in which Big Tech self regulates its compliance with data privacy laws and frameworks, WhatsApp determines not only the substance of its privacy policy but when the contours of that policy are changed. WhatsApp's privacy policy was contingent on the shifting fortunes and interests of WhatsApp and Meta in the context of what was legally permissible, or potentially possible, in the pursuit of maximizing its profit and value to Meta. We start by recalling the scrutiny that WhatsApp and (then) Facebook were placed under by the US's FTC and EU Commission in the lead-up to WhatsApp's acquisition by Facebook in 2014 and subsequent revision of WhatsApp's 2012 privacy policy to document how Facebook and WhatsApp navigated the regulatory landscape to their advantage.

The FTC protects public consumers from unfair or deceptive business practices and the EU Commission enforces the EU's regulatory frameworks; both reviewed the proposed deal with respect to antitrust concerns and sought reassurances that WhatsApp's position with regards to data collection and privacy protections would not be subject to change. Although ultimately approving Facebook's acquisition of WhatsApp, Jessica Rich, FTC's then Director of Consumer Protection, conveyed a strong warning to WhatsApp's General Counsel and Facebook's Chief Privacy Officer that WhatsApp's commitment to consumer privacy must not be undermined by its merger with Facebook:

As you know, both companies collect data from consumers but make different promises and statements with respect to consumers' privacy. ... WhatsApp has made a number of promises about the limited nature of the data it collects, maintains, and shares with third parties -promises that exceed the protections currently promised to Facebook users. We

want to make clear that, regardless of the acquisition, WhatsApp must continue to honor these promises to consumers. (FTC, 2014)

The FTC was referring to WhatsApp's 2012 privacy notice which outlined its collection of certain 'user provided information' including a user's mobile phone number and if applicable, push notification name, billing information and some mobile device information as well as periodic access to user's contact list. WhatsApp informed users that it also collected cookies and logged information when people interacted with its website. And, when using the app itself, WhatsApp collected data on when a message is sent or received, the mobile phone numbers they were sent from and to, and time and date stamps when status information was updated or requested. Significantly, the privacy notice also specified that WhatsApp

does not collect ... names, emails, addresses or other contact information from its users' mobile address book or contact lists other than mobile phone numbers—the WhatsApp mobile application will associate whatever name the WhatsApp user has assigned to the mobile telephone number in his/her mobile address book or contact list – and this occurs dynamically on the mobile device itself and not on WhatsApp's servers and is not transmitted to WhatsApp. (WhatsApp, 2012b)

Although messages were not encrypted at this time, WhatsApp outlined its minimal approach to data collection, specifically that the 'contents of messages ... delivered by the WhatsApp Service are not copied, kept or archived by WhatsApp in the normal course of business' and would only be held on their servers if the recipient was not immediately available online (WhatsApp, 2012a).

Despite warnings by international trade commissions and public reassurance by WhatsApp that it would not change after its sale to Facebook, two options for monetizing WhatsApp were soon being considered by Facebook's senior management which would inevitably place new demands on consumers' data and their privacy. The first concerned publishing targeted ads in WhatsApp's Status feature while the second looked at building tools for businesses to chat with their customers. Brian Acton was not apparently opposed to monetizing WhatsApp per se, though he 'hated targeted ads'. Along with his founding partner Jan Koum, he balked at proposals to use WhatsApp's data to create a unified user profile constructed from data collected across Facebook's companies including Instagram and Facebook messenger and then aggregated and analysed to generate user profiles and drive targeted advertisements (Dwoskin, 2018).

Laying the foundations for extracting some value from WhatsApp data, Mark Zuckerberg overrode the concerns of Acton and Koum to make the

case in mid-2016 that Facebook should have access to WhatsApp's data and integrate some of WhatsApp's and Facebook's services. Facebook's priority was to maximize profit through methods which were at odds with WhatsApp's founding ethos. Afterall, as [Olson \(2018\)](#) reasoned: 'Facebook has one of the world's biggest advertising networks; Koum and Acton hated ads.' While 'Facebook's added value for advertisers is how much it knows about its users; WhatsApp's founders were pro-privacy zealots who felt their vaunted encryption had been integral to their nearly unprecedented global growth.' The demand to monetize WhatsApp at the expense of data privacy principles underscored emergent tensions between Facebook and WhatsApp's founders. Acton glided over their differences when he tactfully articulated that: 'They [Facebook management] are businesspeople, they are good businesspeople. They just represent a set of business practices, principles and ethics, and policies that I don't necessarily agree with' (cited in [Olson, 2018](#)).

The move to integrate Facebook and WhatsApp's technical infrastructure was met with surprise by the EU's regulatory authorities for data protection. Before the deal could close, EU Commission representatives had met with Acton to assess the impact of the transaction on markets for: consumer communications services; social networking services; and online advertising services with respect to consumers in the EU. The subsequent case report summarized WhatsApp's submission, concluding that 'significant engineering hurdles would have to be overcome to enable cross-platform communications' and that, were integration to take place it, 'is likely to result in a significant backlash from both users of Facebook and WhatsApp' who would not want their accounts matched ([European Commission, 2014a](#), p 25).

The EU Commission were reassured. But Acton later recalled in an interview how he 'was coached to explain that it would be really difficult to merge or blend data between the two systems', which he conveyed at the meeting to the EU representatives as well as reassuring the Commission that he nor Koum had any intention of integrating the fundamentally different architecture of Facebook and WhatsApp (cited in [Olson, 2018](#)). It was therefore news to Acton when he subsequently learned that 'people at Facebook' did have 'plans and technologies to blend data'. 'Specifically, that Facebook could use the 128-bit string of numbers assigned to each phone as a kind of bridge between accounts. The other method was phone-number matching, or pinpointing Facebook accounts with phone numbers and matching them to WhatsApp accounts with the same phone number' (cited in [Olson, 2018](#)).

By August 2016 WhatsApp published a revised privacy policy which reflected the new integration of WhatsApp and Facebook's architecture. The latest terms of service were introduced with a renewed commitment to privacy: 'Respect for your privacy is coded into our DNA. Since we started

WhatsApp, we've aspired to build our Services with a set of strong privacy principles in mind' before detailing a significant shift in how data would be shared between WhatsApp and 'Third parties' and importantly between 'Facebook companies'. It was underscored by a new contractual logic between WhatsApp and its users that: 'You share your information as you use and communicate through our Services, and we share your information to help us operate, provide, improve, understand, customize, support, and market our Services' (WhatsApp, 2016c). Moreover, as one of the Facebook family of companies, the privacy policy now stated that WhatsApp users' telephone number and contact list were now shared with Facebook as well as tracking when people last used the service. More specifically,

We may use the information we receive from them, and they may use the information we share with them, to help operate, provide, improve, understand, customize, support, and market our Services and their offerings. This includes helping improve infrastructure and delivery systems, understanding how our Services or theirs are used, securing systems, and fighting spam, abuse, or infringement activities. Facebook and the other companies in the Facebook family also may use information from us to improve your experiences within their services such as making product suggestions (for example, of friends or connections, or of interesting content) and showing relevant offers and ads. (WhatsApp, 2016c)

Woven through the privacy policy and the WhatsApp blog that announced the privacy policy revision was an upbeat future-looking agenda which framed the update as essential innovations for Facebook and WhatsApp to test ways for people to communicate with businesses 'in the months ahead'. As WhatsApp explained, their intention was to find ways of working with businesses on their platform without compromising the simplicity of ad-free WhatsApp:

we want to explore ways for you to communicate with *businesses* that matter to you too, while still giving you an experience without third-party banner ads and spam. Whether it's hearing from your bank about a potentially fraudulent transaction, or getting notified by an airline about a delayed flight, many of us get this information elsewhere, including in text messages and phone calls. We want to test these features in the next several months, but need to update our terms and privacy policy to do so. (WhatsApp, 2016b, emphasis in the original)

The WhatsApp blog also promoted the benefits of 'coordinating more with Facebook' and that WhatsApp users could learn more about 'how to control

the use of your data’ (WhatsApp, 2016b). After first seeing the privacy update notice, existing users had 30 days to opt out of data sharing with Facebook (Gebhart, 2016), while users joining WhatsApp after 25 August 2016 would automatically consent to the new terms. In an interview after his departure from Facebook, Acton presented the 2016 privacy policy update as a compromise between the founders and Facebook’s management who had originally sought ‘broader rights’ to WhatsApp user data. Ultimately, Acton and Koum retained a clause about ‘no ads’, but Facebook did link accounts to present friend suggestions on Facebook and provide its advertising partners with enhanced data insights for their ads on Facebook: ‘WhatsApp would be the input, and Facebook the output’ (Olson 2018). This represented a fundamental rupture in WhatsApp’s approach to data-sharing practices and a move away from WhatsApp’s original commitment to privacy. Just as the FTC and the EU had feared, Facebook would ensure that WhatsApp worked for its profit orientated logics.

WhatsApp made two relatively minor updates to its privacy policy in 2019 and 2020 before announcing another significant revision to its terms of service in early 2021. This update reflected the expansion of WhatsApp’s services to include WhatsApp for Business, a portfolio of business communications solutions for small- and large-scale companies to manage everything from customer services to sales (Business.Whatsapp.com). First launched in January 2018, WhatsApp Business was initially piloted by airline companies to communicate with their customers at scale. In a 2020 quarterly earnings call, Sandberg shared some of the challenges Facebook encountered concerning how they used customers’ data while maintaining that targeted personalized ads were demand led, particularly by smaller businesses:

There is an important debate taking place about the way companies use data, including for online advertising. We welcome this debate and have been advocating for new rules for the internet in a range of areas – from privacy and harmful content to election integrity and data portability. While we face greater scrutiny than ever before, we are also experiencing more demand from businesses for both our free and paid tools – especially our personalized ad products. (Facebook, 2020)

By 2022 the beta testing for WhatsApp Business was underway in India and testing for WhatsApp payments, most notably in Brazil but also India too. WhatsApp business was imagined by Zuckerberg as ‘the next major pillar of our business as we work to monetize WhatsApp and Messenger more’ (Paul, 2022). The 2021 privacy policy ushered in changes to data-sharing practices so that once WhatsApp users engaged with WhatsApp Business, whether as a business or a client/consumer, their accounts would be linked and data shared. WhatsApp informed users that the privacy policy update

was required to provide ‘integrations which enable you to connect your WhatsApp experiences with other Facebook Company Products’ and that they ‘will use your data collected from the app and other Facebook services for content suggestions, people recommendations, and ads along with service improvements’ (WhatsApp, 2021c). Most importantly, for those using WhatsApp Business, it granted WhatsApp licence to share data with third parties. Unlike in 2016 when users had the option to ‘opt out’ of the new terms, in 2021 WhatsApp presented users with a ‘take-it-or-leave-it’ approach. Users could opt out of the new terms but only by deleting WhatsApp.

The trajectory of WhatsApp’s privacy policies and data-sharing practices reflects an incremental departure from Koum and Acton’s minimal data, ‘no ads’ approach, to the integration of WhatsApp and Facebook’s architecture and data sharing and most recently, the introduction of WhatsApp Business as a separate vehicle through which users’ data is shared and monetized. WhatsApp determine the contours and terms of privacy. The 2016 and 2021 updates were presented as essential for improving WhatsApp’s infrastructure and user experiences and were therefore portrayed as inevitable for WhatsApp to innovate and design features for the future.

Petitioning WhatsApp

Data privacy as a public matter

Not everyone was convinced about the necessary and progressive nature of WhatsApp’s privacy policy revisions. Regional regulators, the government of India, internet rights activists, journalists and various publics contested the shifting contours of WhatsApp’s privacy policy through India’s courts and media. Examining the shifting narratives, both the claims and counter claims, alongside media commentaries of these cases reveals much about how privacy is constructed and struggled over for different goals. We ask what the implications of these geolegal debates are for WhatsApp, India and questions of privacy and power.

As the 10-Q narratives indicate, Facebook’s business plan is highly sensitive to the different regulatory parameters imposed on data sharing in different territories. Accordingly, WhatsApp hosts two versions of its terms of service and privacy policy to serve two distinct regulatory landscapes. For users outside of the European Region (that is countries within the European Union) and including India, WhatsApp’s services are provided by WhatsApp LLC which comes under the jurisdiction of US data protection and privacy laws. Whereas for users within the European Region, WhatsApp services are provided by WhatsApp Ireland Limited, ‘which is also the controller of your data responsible for your information when you use the WhatsApp services’ (WhatsApp, 2018c). This detail has implications for the nature and

impact of cases brought against WhatsApp following revisions to its privacy policies as we argue here.

As outlined, the 2016 update represented the most significant shift in WhatsApp's material approach to data collection and sharing through its integration with Facebook's infrastructure. While this update largely went under the radar of a general public – not widely sensitized to the implications of 'data capitalism' (West, 2019) – it did not escape the attention of industry media, privacy activists and regulators, particularly in Europe and India. The EU Commission fined Facebook €110 for 'providing misleading information' about its acquisition of WhatsApp in 2014 (European Commission, 2017). This was disappointing news for Facebook who reportedly gambled that the 'EU might have forgotten because enough time had passed' since WhatsApp made its submissions to the EU Commission ahead of Facebook's acquisition of the company (Acton cited in Olson, 2018). Meanwhile, the Hamburg regulator placed an injunction on Facebook processing WhatsApp data for a period of time, Italy's antitrust agency opened a probe into the fairness of the new terms and the Irish Data Protection Commission launched an investigation which closed in 2021 resulting in a €225 million fine. With the cost of penalties and reprimands appearing not to make a material difference to Facebook and WhatsApp, the risk of compromising legal boundaries appeared to pay off.

In New Delhi, legal challenges against WhatsApp took a different form and emphasis in 2016. Unlike in Europe where the EU Commission designated clear boundaries around data sharing and procedures for protecting user privacy codified in its GDPR, 2018, Indian citizens were not subject to the same privacy rights and data protections. The right to privacy as a distinct fundamental right was an uncertain and emergent legal concept until 2017 while personal data protections were limited to the insertion of a new provision, 43A, into the Information Technology Act in 2008. The patching of an existing act responded to the demands of global companies who outsourced their IT and customer service to India and sought reassurance about the protection, storage and transfer of sensitive personal data in the absence of a formal privacy law in India (Matthan, 2018, pp 116–117).

Rahul Matthan, a lawyer and public advisor on technology and law in India, argues that India has a different 'national experience of privacy' (Matthan, 2018, p 73). In contrast to the US and European experience in the late 1900s, India did not have to confront the same impact of technological shifts and the threat of publicity on personal privacy. Consequently, Matthan argues that privacy was not enshrined as a distinct fundamental right within the Constitution of India despite privacy, as both an idea and practice, being valued within religious, cultural and political life. The UIDAI implementation of India's biometric identity scheme from 2009 proved a watershed moment for privacy imaginaries and rights. The public-private

scheme provoked debates about whether Aadhaar violated an individuals' privacy and who owns, protects and controls the personal data of 1.3 billion Indian citizens. The very existence of Aadhaar presented the possibility of linking personal information with banks, telecom companies, hospitals and schools to understand population and individual level behaviours concerning communications, finance, education, health and much more (Sudhir and Sunder, 2020). Under the 2017 Puttaswamy ruling on the 'right to privacy' was enshrined in the Indian Constitution but its implications with respect to data protection and privacy rights were yet to be codified (see Chapter 2). That would remain subject to considerable debate for the foreseeable future, with implications for the cases we examine next.

In contrast to the 2016 update, WhatsApp's 2021 privacy policy update sparked far greater public scrutiny and media attention, particularly in India (India Today Tech, 2021; New York Times, 2021). Here, WhatsApp users and civil society organizations were more alive and attentive to questions of data privacy following the public activism and litigation around the implementation of Aadhaar and resulting Puttaswamy judgement concerning the constitutional 'right to privacy'. By now, privacy had become a public matter in India. Globally too, the disclosures of Edward Snowden, the ex-CIA technical advisor and now privacy activist, revealed the close relationships between international governments and telecommunications companies in the operation of global surveillance programmes by the National Security Agency (NSA) and Five Eyes intelligence alliance while revelations later emerged concerning the alleged use of personal data by Cambridge Analytica to influence election behaviour. These disclosures had produced a newly cynical and cautious global and Indian public concerning the use of their personal data for surveillance and data capitalism.

Litigating privacy: privacy rights and competition

Against this backdrop in India three intersecting threads of litigation coalesced around questions of WhatsApp, data privacy and the Government of India in the wake of its 2016 and 2021 privacy policy updates. In the first two sets of proceedings, citizen and lawyer advocates and the Competition Commission of India respectively contested the 2016 and 2021 privacy policy updates in which WhatsApp is the respondent claiming that they violate the privacy rights of Indian citizens. In the third strand of litigation, WhatsApp is the petitioner and has moved to sue the Government of India over its new Information Technology Rules which require 'significant social media intermediaries' to 'trace the first originator of a message' (Ministry of Electronics and Information Technology, 2021). In this case, WhatsApp claims that the traceability requirement is unconstitutional and violates people's right to privacy guaranteed under the Supreme Court's Puttaswamy

judgement (Agrawal, 2021). We examine the third thread in the final section of the chapter.

We set out the first of these threads here, and for which the initial challenge to WhatsApp's 2016 privacy policy came from Indian citizens and childhood friends – Karmanya Singh Sareen and Shreya Sethi – whose legal networks and personal motivation enabled them to pursue their case before the Delhi High Court. In our interview with Karmanya Singh Sareen, now a patent lawyer based in New Delhi, he described how in 2016 he was studying for an engineering degree at Imperial College London and was really 'into data privacy'. Karmanya regarded WhatsApp as 'the ideal start up'; he was particularly impressed by the company's pro-privacy origins and respected the founders for figuring out how to make messaging work over the internet. The 2016 privacy policy revision (after Facebook's acquisition of WhatsApp) felt wrong to him, and a betrayal of WhatsApp's 'privacy promise'. With the support of his network and a friend of his, Shreya Sethi, who was then a law student, they took the matter to the Delhi High Court and then the Indian Supreme Court. For Karmanya, this was a 'purpose driven project'. He was keen to emphasize that he did not despise WhatsApp, to the contrary he had long been a supporter and respected WhatsApp's ambition to commercialize their product. But he was concerned about how the tech company could access and monetize users' data in the context of India's limited legal and material protections around the right to privacy. At the time, the right to privacy was not recognized as a fundamental right, but variously and subsequently declared as a fundamental right under Article 21 with respect to the right to life and personal liberty.

In 2016, 'privacy hadn't been crystallized as a right' and so Karmanya reasoned that taking just WhatsApp to court 'would not have been the best strategy because they would have defended themselves by saying that they were operating within the law'. Instead, on the advice of his lawyers, Karmanya filed a writ petition against the Union of India as well as WhatsApp (and Facebook – now Meta) before the Delhi High Court to protect the rights of WhatsApp's users (*Karmanya Singh Sareen & Anr v Union of India & Ors*, W.P.(C) 7663/2016). The writ was 'filed in [the] public interest on behalf of themselves and millions of users who are citizens of India using "WhatsApp" messaging service'. The initial petition was granted partial relief by a division bench of the Delhi High Court, which declared that WhatsApp cannot use the data, as per the 2016 privacy policy, of those users who cease use of WhatsApp. The bench also directed WhatsApp to delete the data of all such users, for the period up to 25 September 2016, which was the effective date on which the 2016 privacy policy came into force.

Not satisfied with the partial relief, whereby WhatsApp was permitted to proceed with the new privacy policy from September 2016 onwards for

the data collected post September 2016, Sareen and Sethi filed a Special Leave Petition (SLP) [*Karmanya Singh Sareen & Anr v Union of India & Ors*, SLP(C) 804/2017] before the Supreme Court against the Delhi High Court's judgment. This is a legal mechanism which can be exercised when any substantial question of law is involved or a gross injustice has been done, and is for the Supreme Court to exercise its extraordinary jurisdiction. The Petitioners impleaded, in addition to the UoI, WhatsApp and Facebook, the TRAI, under the Ministry of Communications, to articulate an urgent need to protect the personal data of Indians who use internet messaging applications such as WhatsApp. The Petitioners argued that data-sharing practices with 'Facebook and all its group companies for the purposes of commercial advertising and marketing' threatened the right to privacy of WhatsApp's Indian users. The 2016 privacy policy

sought to alter /change the most valuable, basic and essential feature of this internet-based messaging service, by unilaterally threatening to take away the protection to privacy of details and data of its Users and sharing the same with Facebook and all its group companies including for the purpose of commercial advertising and marketing. (Singh Sareen, 2017, p I)

A 5-Judge Constitution Bench led by Justice K.M. Joseph heard the case in 2017 over two days which included an intervention from the Internet Freedom Foundation (IFF), a non-profit organization that promotes the rights of Indian internet users particularly around freedom of speech, privacy, net neutrality and freedom to innovate. In response to the Union Government's request and WhatsApp's agreement, the bench decided to postpone the judgment until *after* India's then called 'Digital Data Protection Bill' came into force, to avoid contradictions arising. After WhatsApp introduced further updates to its privacy policy in 2021 requiring users to accept the new terms of service before 28 February 2021, Karmanya Singh Sareen filed another application under his existing case claiming that WhatsApp offered lower privacy protections to Indian citizens compared to European citizens. Additional cases were also brought, including a writ petition before the Delhi High Court in 2021 by litigation lawyer, Chaitanya Rohilla (*Chaitanya Rohilla v Union of India & Others*, 2021). Rather than petition TRAI as Sareen and Sethi had done, this petition requested that the court 'lay down guidelines' under Section 79(2)(c) read with Section 87(2)(zg) of the Information Technology Act to prevent WhatsApp from sharing any user data with Facebook or any other third parties.

After a lengthy pause, in part due to the COVID-19 pandemic, the *Karmanya Singh Sareen v Union of India* was listed for a hearing on 29 September 2022 (*Petition for Special Leave to Appeal (C) No.804/2017*). The

respondents – WhatsApp and Facebook and the Union of India – requested a further delay until the government enact a data protection law. On 31 January 2023 the respondents sought another deferment. By now the Digital Personal Data Protection Bill, 2022 had been drafted and was due to be tabled before Parliament in the 2023 budget session and potentially decreed by the end of April. The Supreme Court proposed otherwise that final arguments should be scheduled despite the draft DPDP Bill 2022. But efforts to find a mutually agreeable date between the counsel of the respondents proved difficult and the Supreme Court had no choice but to defer the hearing until 11 April 2023 (Singh, 2023). However, until a new hearing could take place, the Supreme Court directed WhatsApp to ‘publish a disclaimer in five popular newspapers that its users can continue using the app even if they do not accept the new privacy policy’ (PTI, 2023; Spandana and D’Souza, 2023). The case is still pending.

The second thread of legal action, in which WhatsApp (and Facebook) are the respondents challenges the privacy policy updates from the perspective of competition and antitrust in which the state is mobilized to curtail corporate power and protect the interests of consumers. Vinod Kumar Gupta, a chartered accountant, filed an order in 2016 on behalf of the Fight for Transparency Society. This focused on whether WhatsApp was indulging in ‘predatory pricing’ and abusing its ‘dominant position in the market’. Vinod Gupta claimed that with WhatsApp backed by funds from Facebook the messaging platform was able to drop its minimal subscription fee and substantially grow its user base. With no option to opt out other than deleting WhatsApp, users were thus compelled to give their ‘so-called consent’ to the privacy policy update and share their details with Facebook if they wished to continue using the service. At that time the Competition Commission of India dismissed the complaint concerning WhatsApp’s abuse of dominance under the Section 26(2) of the Competition Act, 2002 (Competition Commission of India, 2002). The Commission argued that users could ‘opt out’ of the privacy policy update by deleting their account and that there were ‘no significant costs preventing the users to switch from one consumer communication apps to another’.

In 2021, considering media reports and the potential impact of the Policy and Terms for WhatsApp users and market, the Competition Commission of India issued a *suo moto* investigation under section 26(1) of the Competition Act, 2002 (Competition Commission of India, 2002). Concerned with the privacy policy update from an anti-competition perspective, the order took issue with two overlapping concerns; first, that WhatsApp could share users’ personalized data with Facebook companies, and second, that ‘users will have to mandatorily accept the new terms and policy in their entirety including the terms with respect to sharing of their data across all the information categories with other Facebook Companies’. Referencing the earlier Vinod

Gupta case, the Competition Commission of India (CCI) observed that in the 2016 privacy policy update ‘WhatsApp had provided an option to its users to “opt out” of sharing user account information with “Facebook” within 30 days of agreeing to the updated terms of service and privacy policy.’ In contrast the 2021 privacy policy update presented users with the decision to ‘take-it-or-leave-it’. The CCI also incorporated the IFF’s ‘expert information’ into the main case which the non-profit reported as ‘a huge opportunity to present the user’s point of view to the Commission!’ (T. Singh, 2021).

In 2022 the Delhi High Court rejected the appeals made by WhatsApp and Facebook to maintain that parallel inquiries by two separate authorities in respective fields of law did not preclude the possibility of both being heard in court. In 2024 the CCI’s investigation concluded that ‘the 2021 policy update forced users to accept more intrusive data collection practices, leveraging the company’s significant market position’ (Naman Kumar, 2025) and imposed a penalty of Rs.213.14 crore (CCI, 2024). Meta swiftly moved to appeal the verdict (Meta, 2025).

Questioning the idea of consent, choice and control

‘Indulging in anti-user practices’

A running theme of the legal materials challenging WhatsApp’s privacy policy updates concerned how users were notified of the changes to WhatsApp’s privacy policy and the degree to which user consent and choice was meaningfully articulated. WhatsApp users were first alerted to the 2021 privacy policy update by a ‘pop up’ when opening WhatsApp with the headline ‘WhatsApp is updating its terms and privacy policy’ followed by a series of bullet points highlighting the ‘key updates’.

The ‘key updates’ pertained to how WhatsApp processes user data, how businesses use Facebook services to manage WhatsApp chats and how WhatsApp’s digital infrastructure is integrated with other Facebook company products such as Facebook, Instagram and Facebook messenger. After citing its headline changes, the pop up sought to influence users to click the only option available, a large blue button citing ‘Agree’ to the ‘new terms and privacy policy’ before moving into the main app, or else hit a more discrete ‘X’ sign in the top right hand of the screen. All users had to ‘Agree’ by 8 February 2021 ‘to continue using WhatsApp’. A further option was available, as WhatsApp indicated ‘if you would prefer to delete your account and would like more information’ ... ‘you can also visit the Help Centre’. In an affidavit to the Delhi High Court, the Ministry of Electronics and Information Technology surmised that ‘it appears that consent to sharing and integration of user data with other Facebook Companies for a range of purposes including marketing and advertising, has been made a precondition for availing WhatsApp service’ (Competition Commission of India *Suo Moto Case No. 01*, 2021).

The condition that users had to opt-in to continue accessing WhatsApp's service did 'not provide the users with the option to opt-out of their data being shared with Facebook Inc, WhatsApp's [sic] parent company' (SCO, 2021). Moreover, the repetition of notifications targeted at users still to 'Agree' and the persistent nudge to click the central, large blue 'Agree' button instead of a much smaller more marginal 'x' reflected what Harry Brignull calls 'dark pattern' design. That is, 'a manipulative or deceptive trick in software that gets users to complete an action that they would not otherwise have done, if they had understood it or had a choice at the time' (Brignull, 2021). Thus, the Ministry of Electronics and Information Technology claimed that WhatsApp was 'indulging in anti-users practices by obtaining "trick consent" from users for its updated privacy policy ...' That data sharing was not 'fully transparent nor based on voluntary and specific user consent, appears prima facie unfair to users' (*Competition Commission of India Suo Moto Case No. 01, 2021*).

In our interview with Bishakha Datta from the NGO, Point of View they underscored the power imbalances that existed with WhatsApp's approach to accessing user consent, stating that it is 'meaningless if you can't say no without consequences'. While users could initially refuse to consent to the changes in the privacy policy, WhatsApp persistently asked users to 'agree' with repeated pop ups. Datta contended that it was important to reframe WhatsApp's behaviour to users as a form of harassment.

I think if you were an individual and WhatsApp was another individual, I would be like: Why is this person going on bothering me all the time when I've said no? So, I think sometimes when we think of consenting, like human consent, it helps us recalibrate our expectations of consent from apps and, like, from platforms. If this was a human being [behaving] with me [in this way] ... forget it.

In his 2016 petition, Karmanya Singh had earlier raised concerns that while the information might be shared by WhatsApp to ensure informed consent 'the manner in which so-called consent was sought to be taken [was] highly deceptive in as much as almost the entire community of Users of WhatsApp in India are not equipped to even read, much less comprehend, the consequences' of the Terms and Conditions. 'WhatsApp is pretending to obtain [sic] consent of the Users' (*Karmanya Singh Sareen v Union of India, SLP*). The extent to which privacy policies can be meaningfully engaged with by *all* users was also raised by the Competition Commission of India in 2021, citing that users are 'entitled to be informed about the extent, scope and precise purposed [sic] of sharing of ... data by WhatsApp with other Facebook Companies' but the 'information categories' within the Privacy Policy as well as the terms of service were 'too broad, vague and unintelligible'. (*Competition Commission of India Suo Moto Case No. 01, 2021*)

For instance, it is not clearly defined what is meant by how ‘users interact with others (including businesses)’ and what would constitute ‘service-related information’ or ‘mobile device information’. Malavika from IT for Change agreed:

I read it [the privacy policy], actually ... after a point [it] was so overwhelming for an individual user. If I wasn’t a lawyer-researcher but just someone using WhatsApp, I would be really exhausted after reading it. I really needed to use WhatsApp. So, I just said ‘okay’ to it. And I know that almost 80 per cent of the people I spoke to also did the same. But had I said ‘no’, then I wouldn’t have been able to use it. So yeah, I wasn’t really given a choice. And this is the issue with privacy policies ... You’re not really given a choice when it pops up.

Malavika has a point, WhatsApp’s privacy policy has become incrementally longer and more complex since 2012. According to the Flesch-kincaid readability test, the 2021 update takes almost 14 minutes to read, is categorized as ‘difficult to read’ and presumes a college-level education to understand its meaning. For an average internet user, WhatsApp’s privacy policy is just one of many that they would have encountered for digital services and websites and been compelled to consent to in return for access. One study contended that if an average American user read all the privacy policies they encountered it would take individuals 201 hours per year to read them at a national opportunity cost of \$781 billion to the economy in lost time (McDonald and Cranor, 2008, p 2). Privacy policies are not for users, they are for lawyers.

The petitioners argued that not only was consent not meaningfully engaged by WhatsApp but that any notion of ‘choice’ was meaningless within India’s social and economic context; users had little choice but to agree to the new terms of service or lose access to the messaging app. The CCI called out the unfair advantage being gained through WhatsApp’s ‘network effect’ that ‘ensures that customers do not switch to other platforms easily unless there is a new competitor entering the market with an altogether disruptive technology’ (*Competition Commission of India Suo Moto Case No. 01, 2021*). The Government of India also weighed in on the issue and publicly reiterated the case of the CCI ‘that the unilateral changes to the WhatsApp Privacy Policy undermine the privacy, autonomy and freedom of choice of Indian citizens’ (*Harsha Gupta v WhatsApp & Ors, 2021*). In this context, ‘the “all-or-nothing”/ limited functionality leading to complete withdrawal of service’ approach adopted by WhatsApp takes away meaningful choice from Indian users and undermines the spirit of the landmark judgment of the Supreme Court of India in Puttaswamy (*Harsha Gupta v WhatsApp & Ors, 2021*). Moreover, given WhatsApp’s market dominance in India, this

necessarily meant that users would give up their access to important private digital messaging spaces.

In practice, it was argued that ‘a façade was being created as if a consent is being taken from the Users’ (*Karmanya Singh Sareen & Anr v Union of India & Others, Special Leave Petition*, 2017). Chaitanya Rohilla’s petition put it more forcefully that ‘WhatsApp has put the Sword of Damocles upon its users, compelling them to share their data to them and ultimately other companies. This type of dissemination [sic] of information about an individual involves high risk of misuse of that data’ (*Chaitanya Rohilla v Union of India & Others*, 2021). The CCI questioned why WhatsApp users could not have more control of their data and recalled that in 2016 users could at least opt out of data sharing with Facebook without compromising their access to the service.

Under competitive market condition, users would have sovereign rights and control over decisions related to sharing of their personalised data. However, this is not the case with WhatsApp users and moreover, there appears to be no justifiable reason as to why users should not have any control or say over such cross-product processing of their data by way of voluntary consent, and not as a precondition for availing WhatsApp’s services. (*Chaitanya Rohilla v Union of India & Others*, 2021)

In response to these claims WhatsApp consistently defended their policy amendments in 2016 and 2021 by furthering the narrative that all users are autonomous consenting individuals, as they put it: ‘Users have willingly signed agreements, which is therefore a consensual contract’ (*Karmanya Singh Sareen & Anr v Union of India*, 2016). Moreover, users are not coerced into using the app and can opt out at any time. As WhatsApp’s counsel argued in an affidavit: ‘we have taken note of the fact that under the Privacy Policy of “WhatsApp”, the users are given an option to delete their “WhatsApp” account at any time, in which event, the information of the users would be deleted from the servers of “WhatsApp”’ (*Karmanya Singh Sareen & Anr v Union of India*, 2016).

Privacy policy fiction

As WhatsApp argued in its defence, users’ agreement to their privacy policy was a ‘consensual contract’: a socio-legal contract to which users give their digital consent for their data to be collected by WhatsApp, and in some cases, shared with Third parties. Within social relationships of asymmetrical power, giving informed consent is posited as an important ethical mechanism that ensures individuals have access to comprehensive information and knowledge to empower individuals to make choices over their bodies and lives. As a social-legal contract, consent draws on western philosophy and

‘has been introduced in various spheres of life ... for people to have more control, agency and autonomy on their bodies and lives’ (Carmi, 2021, p 3). Yet, as the petitioners infer in their objection to the mode and manner of the privacy policy updates, the application and meaning of consent in the context of data and digital privacy operates within a different environment and with different implications; digital consent is not only a façade it is also ‘flawed’ (Carmi, 2021, p 15). Rather than combating asymmetrical power relations between individuals and Big Tech, we argue that WhatsApp (like other tech companies) mobilizes users’ consent to its privacy policy ‘contract’ to advance and defend the company’s power. The fantasy of consent performed through the privacy policy and the data points collected by users feeling compelled to hit the big blue button ‘Agree’ is a form of ‘legal entrepreneurialism’ that permits Big Tech access to our data ‘property’.

WhatsApp entrenches its power through digital consent by furthering three interlinked aspects of this fantasy that: (1) privacy contracts are fair and equal; (2) users are sovereign and autonomous individuals; and (3) digital consent, choice and control empowers users. First, stressing the significance of users’ consent for privacy rights rests on the erroneous belief that privacy policies as a socio-legal contract between WhatsApp and its users fairly protects privacy and data rights. Drawing on feminist philosophy, Weinberg (2017) argues that ‘[p]rivacy rights, in their emphasis on the individual’s proprietary ownership over privacy, foster the sense that freedom is achievable through contract and ownership’ (Weinberg, 2017, p 13). By formalizing the social practice of making and keeping agreements, contracts ensures a degree of predictability and clarity concerning an expectation that rights and obligations will be fulfilled by respective parties. Though they may promise a degree of equality, Weinberg demonstrates by drawing on Pateman how ‘a Contract always generates political right in the form of relations of domination and subordination’ (Pateman, 1988, p 8 cited in Weinberg, 2017).

In the context of ‘surveillance capitalism’ (Zuboff, 2018) the subject of consent shifts from users agreeing to participate in a relationship of exchange to themselves becoming the product or the message that is communicated as data (Carmi, 2021). Relations between users and Big Tech are defined by extractive processes that produce big data to be aggregated and analysed by machines in the generation of new value for profit. Participation in digital life therefore depends on a user’s consent to share data which can be transformed in this way. Where workers sign contracts agreeing to their compliance with employers, Weinberg argues that ‘privacy rights put the subject in the position of either agreeing to be exploited, or to not participate in digital culture’ (2017, p 13).

Understanding ‘surveillance capitalism’ as the product of lawlessness, Zuboff contends the normative social-legal relationships that constitute

the contract such as collaboration, keeping promises and maintaining equal respect, have been substituted or bypassed by Big Tech's 'uncontracts'. 'Uncontracts' are one-way processes underpinned by forced 'agreements' that demand 'perpetual compliance' (Zuboff, 2018, pp 334–336), which can be amended any time at the behest of the technology company's interests. Cohen (2019b) on the other hand interprets the adoption of the private contract between Big Tech and individuals as a form of 'legal entrepreneurialism' that is at least seen to protect the users' data as property.

Second, WhatsApp's privacy policy depends on western liberal democratic principles of user sovereignty to structure privacy rights where individuals make autonomous choices and are equally able to enter contracts. Yet, the feminist and post-colonial critique is that western liberal democratic discourse has failed to create, and more often undermined, the equality for all individuals. The idea of the sovereign individual conceals and perpetuates the exploitation of contractual relations and the exclusion of gendered, minoritized and colonized individuals. In addition, the structuring of privacy rights as a solely individual concern is in blatant contradiction to Meta's corporate ambitions to enhance WhatsApp's worth by expanding its user network based on connections and sharing. Hence, WhatsApp does not value its users as sovereign individuals; it values its users as inherently networked individuals. As Myers-West argues, 'data capitalism ... places primacy on the power of networks by creating value out of the digital traces produced within them' (West, 2019, p 2). The metadata on how, when and from where individuals connect and share with others on the network is WhatsApp's principal source of value. Moreover, private and public life are increasingly indivisible. The option for users who dissent from the new terms to 'opt out' is disingenuous of WhatsApp given its existing market share in India and ambitions for ubiquity as a digital utility. The implication is that those unwilling to trade their metadata for access to digital private messaging spaces are denied their right to private digital messaging in a network that matters.

Third, a western liberal approach to privacy as consent confers the misleading idea that individuals have choice and control over their data within digital ecosystems. In practice, consent normalizes data capitalism as inevitable and places the responsibility on to individuals to determine their privacy needs in contexts of inadequate knowledge. Carmi argues that 'digital consent is used as a mechanism that transfers data and hence profits to companies while shifting the responsibility of harm to the citizens' (Carmi, 2021, p 15). For Weinberg this means that 'the impetus is on users to perform autonomous self-management and cultivate the skills and literacy necessary for determining whether to engage with certain services and platforms' (Weinberg, 2017, p 10). Conversely, users who do not educate themselves about their privacy rights and technology company

practices only have themselves to blame for potential privacy violations (Gehl, 2016). Even individuals with the capacity and commitment to understanding their rights implications of data and privacy policies cannot possibly know the full extent of data processing, aggregation and decontextualization for '[t]he forms of "knowing" associated with big data mining are available only to those with access to the machines, the databases, and the algorithms' (Andrejevic, 2002, p 1676 see also Solove, 2013; Zuboff, 2019). Consent to privacy policies is treated as a one-off event, in which 'Your continued use of the WhatsApp Site and WhatsApp Service constitutes your agreement to this Privacy Policy and any amendments' (WhatsApp, 2012a). Whereas feminist critics have contrasted the application of consent in digital environments to other socio-legal contexts, for example sexual relationships, to argue that digital consent should acknowledge the ongoing need for consent in response to changes in environment or information, as determined by *both* parties and not only by the dominant partner, in this case WhatsApp. Moreover, as Bishakha Datta highlighted, WhatsApp's digital architecture of consent denied a user's refusal to consent that, within a social relationship, would amount to harassment.

Waldman is highly critical of the ways that 'consent is easy to manipulate and manufacture' within 'coercive bureaucracies' (Waldman, 2021, p 56) and in particular the 'conflation of consent with real choice' by corporations (Waldman, 2021, p 55). Waldman concludes that '[i]n the end operationalising consent in the privacy space achieves the exact opposite of individual control and empowerment' ... the information industry 'take[s] refuge in consent' to absolve them of their data protection responsibilities because 'consent legitimises nearly every form of collection, use or disclosure of personal data' (Solove, 2013, p 1880; Waldman, 2021, p 57). The fiction of digital consent is not just a place for WhatsApp to hide from responsibility but is used to advance WhatsApp's private power vis-à-vis its citizen-users and the Indian government. But as we show, the fiction of the privacy policy is being contested and reimaged through legal spaces. These debates are also questioning the nature of data relations between WhatsApp and India.

Geolegalities of digital privacy regulations

Debates concerning the limits of consent and choice centred the relationship between WhatsApp and its users, between Big Tech and citizens. The court documents and related privacy discourse and public debates also evoked geolegal dimensions – which read through a feminist lens concern how 'law intermeshes with intimate corollaries of geo-politics and geoeconomics' (Brickell and Cuomo, 2019, p 104). These contentions evoked the

nation state and its shifting data relations with WhatsApp in several ways concerning: first, the articulation of private corporate power; second, India's data and national sovereignty; and finally, how Big Tech (and the state's) legal strategies and entrepreneurship are productive of space and time in the context of privacy regulations.

First, in justifying the significance of their cases, petitioners and representatives asserted that although WhatsApp was a private authority motivated by profit, it had 'public power' and therefore a responsibility to the public. The 'public power' of WhatsApp was illustrated by Mr Harish Salve, representing Karmanya Singh Sareen who used the analogy of '[a] teacher raising a hand to stop traffic while her students cross the road' to explain that they exercise 'public power'. 'Similarly, telecom companies exercise public power even if they are motivated by commercial purposes. Entities and companies may have commercial motivations, but if they provide a public service, they can and must be regulated' (SCO, 2017a). In 2021, Chaitanya Rohilla's submission emphasized how WhatsApp had proven to be 'an effective alternative to SMS' and 'grown its root deep into the society' (*Chaitanya Rohilla v Union of India & Others*, 2021, point 3). Moreover, WhatsApp has not only 'become an important mode of communication amongst the citizens of India' but it 'is also being used to aide multiple Governmental functions as well including within the Supreme Court to communicate summons and elsewhere to host legal mediations'. Rohilla claimed that 'This substantiates to the fact that WhatsApp is discharging a Public Function despite being a private entity' and therefore 'WhatsApp cannot be allowed to go berserk at its whims and fancy' (*Chaitanya Rohilla v Union of India & Others*, 2021, point 6).

Moreover, summaries of court proceedings reveal that the private nature of WhatsApp's authority and infrastructures presented a challenge to existing laws in holding them to account over concerns about data and privacy rights. For instance, in response to the Karmanya Singh Sareen case, the court noted that WhatsApp's terms of service amounted to a 'private contract' and were not governed by any statutory provision and were thereby not amenable to the writ jurisdiction under Article 226 of the Constitution of India (see Chowdhury, 2018, p 449). Again, in 2021 Justice Sanjeev Sachdeva was ultimately dismissive of Rohilla's case, arguing that WhatsApp is a 'private app', and should anyone have a problem with WhatsApp's terms he or she can remove the app from their phones (Banka, 2021).

To absolve itself of responsibility, Facebook appealed to the Delhi High Court against its implication in both the citizen-led and the CCI cases. By presenting Facebook as a private and decentralized company it contended that it should not have been made a party to the case alongside WhatsApp. During the 2017 proceedings the Supreme Court Observer recorded that

Mr Arvind Datar, representing Facebook, began by clarifying that although Facebook has acquired WhatsApp, ‘not a single comma or word’ has been shared between them so far, or will be shared in the future. Mr Sibal, representing WhatsApp, went further and said that he is ready to have a statement recorded to that effect. (SCO, 2017a)

In the 2022 Delhi High Court case brought by the Competition of India against WhatsApp and Facebook Mr Mukul Rohatgi, the advocate representing Facebook insisted that the subject of investigation is WhatsApp and that although Facebook is a ‘common owner, it would not mean that they are required to share the burden’. Moreover, he stated that the 2016 and 2021 policies under scrutiny are not Facebook’s but rather WhatsApp’s policies and that ‘just because information can be shared by virtue of those policies, it is not a ground to investigate into the affairs of Facebook’ (*WhatsApp LLC v Competition of India & Anr*, 2022).

The Delhi High Court rejected Facebook’s claim that its data was siloed and activities decentralized as Mr Singh, representing the CCI emphasized that Facebook was a ‘group company as well as the holding company of WhatsApp’ (*WhatsApp LLC v Competition of India & Anr*, 2022). The Chief Justice, Subramonium Prasad, reasoned that

one of the key issues with the 2021 Policy is its [WhatsApp’s] propensity to share the data of its users with Facebook Inc., the parent company of WhatsApp. Solely for the reason that the policies itself do not emanate out of Facebook Inc., the Appellant cannot hide behind the fact that it is the direct and immediate beneficiary of the data sharing mechanism envisaged by the policies.

As such, Facebook’s presence was necessary as ‘a proper party in the investigation pertaining to the 2021 Policy and the alleged anti-competitive practices they trigger’ (*WhatsApp LLC v Competition of India & Anr*, 2022).

Maha Ravi Atal’s (2021) arguments are insightful here for considering how platform companies ‘deliberately and consciously mask’ their ‘deeply centralised model of power’ by ‘cultivating the impression of decentralization’. Doing so affords them a degree of ambiguity and potential to challenge regulatory law and ‘thwart both rhetorical and regulatory challenges to their power’ (Atal, 2020, p 338). We argue that Facebook’s appeals against its involvement are consistent with the strategies of Big Tech companies seeking to evade responsibility (and in part, as we suggest later in the chapter, delay court proceedings). In this case, Facebook’s attempt to hide behind its status as a private corporation independent of WhatsApp, was thwarted by the courts. Although as we show, the private nature of WhatsApp’s contractual relationship with its users impeded the court’s authority to intervene under existing privacy laws.

Second, legal petitions as well as government and media narratives lamented the opportunity that uneven privacy regulations had presented for a foreign owned technology company to unfairly exploit Indians' data and undermine the nation's sovereignty. The contention in 2016 and 2021 was that an American online social media and social networking service based in Menlo Park, California was collecting and sharing Indian's data and taking advantage of India's weaker data protection laws to further its economic interests. Karmanya Singh Sareen filed the petition against the Government of India in the 'public interest' concerning 'the absence of any regulatory framework and in view of the clear and present danger and threat to the rights of millions of citizens who use WhatsApp'. He compelled the High Court to recognize the state's responsibility 'to guarantee and ensure the protection of the personal and private data and information of these millions of citizens' (*Karmanya Singh Sareen & Anr v Union of India & Others Special Leave Petition*, 2016).

Karmanya Singh Sareen's petition aimed to illustrate India's inadequate response which protected the data of users before 25 September 2016, but not those after the privacy policy update by highlighting the 'proactive action' taken within other jurisdictions such as the UK, Germany, EU group of nations and 'even in the United States' to restrain WhatsApp 'from sharing data belonging to Users' (*Karmanya Singh Sareen & Anr v Union of India & Others Special Leave Petition*, 2017). This argument was reiterated when the Supreme Court requested the Government of India and WhatsApp to reply to a fresh plea alleging lower standards of privacy for Indians in comparison to European users saying it is the duty of the judiciary to protect citizens' privacy. It directly confronted WhatsApp, saying that 'You may be \$2–3 trillion company but people's privacy is more valuable for them and it is our duty to protect their privacy' ([TimesofIndia.com](https://timesofindia.com), 2021).

Relatedly, the question frequently raised concerned the implication of WhatsApp's ownership of Indians' data for national sovereignty. Summarizing the Delhi High Court judgement, 2017, Mrs G. Rohini Chief Justice noted that while WhatsApp claimed to set up 'a unique profile of providing complete protection of privacy policy', the 2012 Privacy Policy contained a specific clause about the transfer of data to the US:

Special Note to International Users: The WhatsApp Site and Service are hosted in the United States and are intended for and directed to users in the United States. If you are a user accessing the WhatsApp Site and Service from the European Union, Asia, or any other region with laws or regulations governing personal data collection, use, and disclosure, that differ from United States laws, please be advised that through your continued use of the WhatsApp Site and Service, which are governed by California law, this Privacy. Policy, and our Terms of

Service, you are transferring your personal information to the United States and you expressly consent to that transfer and consent to be governed by California law for these purposes.

This clause served to protect WhatsApp's data interests and limit the powers of other jurisdictions. Chaitanya Rohilla's petition following the 2021 update questioned such cross-border data-sharing practices when arguing that in addition to making a 'mockery out of our fundamental right to privacy while discharging a public function in India', WhatsApp 'was jeopardizing the National Security of the country by sharing, transmitting and storing the users data in some another country and that data in turn will be governed by the laws of that foreign country' (*Chaitanya Rohilla v Union of India & Others*, 2021). WhatsApp's move to deepen its data collection and sharing practices was therefore seen as a challenge to India's data sovereignty and an affront to India's democracy more generally: 'This type of arbitrary behaviour and brow beating cannot be accepted in a democracy and is completely ultravires and against the fundamental rights as enshrined in the Constitution of India' (*Chaitanya Rohilla v Union of India & Others*, 2021). In a later letter to WhatsApp from the Ministry of Electronics and Information Technology it reiterated this position, stating that 'The government of India owes a sovereign responsibility to its citizens to ensure that their interests are not compromised' (M. Singh, 2021).

Third, as the socio-legal lives of WhatsApp's privacy policy came to life through its amendments and ensuing debates, their legal (re)drafting and defence was, or was at least perceived to be, productive of space and time. In our interview with Karmanya Singh, he emphasized that the reason they took the Indian government as well as WhatsApp to court was 'because privacy hadn't been crystallised at the time [2016] as a right'. WhatsApp would have simply said that 'they were following the law'. As Karmanya explained in an interview to us, for WhatsApp, 'laws are just constraints'; WhatsApp would be looking to see where and how it is possible for them to operate. He furthered that '[f]or Meta, data is its biggest currency, as well as asset. WhatsApp will be looking at the optimal ways to make a profit while complying with the law. It is a balance.'

In the application filed before the Supreme Court by Karmanya in *Karmanya Singh Sareen & Anr v Union of India & Ors* in January 2021 (against another updated version of WhatsApp privacy policy), he responded to WhatsApp's privacy policy update by drawing attention to the boundaries of WhatsApp's privacy policies, its scope of application, who was included and who was excluded, and the uneven global privacy landscape. His key claim was that WhatsApp was offering 'lower care and protection to [Indian] users' privacy and rights' compared to users in European countries. (SCO, 2021). Chaitanya Rohilla made a similar case:

The updated Privacy Policy introduced by WhatsApp won't be applicable for the European Region owing to the data protection law in place there. WhatsApp is legally bound to not share data with Facebook in the European Region because it's a contravention of the provisions of the General Data Protection Regulation (GDPR). GDPR is a regulation in the European Union law on data protection and privacy in the European Union and the European Economic Area. WhatsApp and in turn Facebook is trying arbitrarily and in most monopolistic way to enforce it in India as they see vulnerability in the absence of any comprehensive law in this subject. (*Chaitanya Rohilla v Union of India & Others*, 2021)

The fact that India was subject to different privacy policies was not refuted, after all since 2018 WhatsApp has operated two different privacy policies to ensure it complies with Europe's more stringent data privacy regulatory environments. In a statement to Forbes, a WhatsApp spokesperson confirmed that the changes to WhatsApp's data-sharing practices would not apply in Europe and the UK and that '[f]or the avoidance of any doubt, it is still the case that WhatsApp does not share European Region WhatsApp user data with Facebook for the purpose of Facebook using this data to improve its products or advertisements' (Page, 2021). In a letter from the Ministry of Electronics and Information Technology to WhatsApp later that year the government minister insisted that Indian citizens (and their data) should not be exploited and regarded with any less respect than users in Europe: 'As you are doubtlessly aware, many Indian citizens depend on WhatsApp to communicate in everyday life. It is not just problematic, but also irresponsible, for WhatsApp to leverage this position to impose unfair terms and conditions on Indian users, particularly those that discriminate against Indian users vis-à-vis users in Europe' (PTI, 2021).

While the privacy policy update also pertained to regions other than India, the implementation of the new privacy policy before the widespread rollout of WhatsApp Business in India appeared to signal its particular significance for WhatsApp in India and the data monetizing opportunities afforded by India's weaker data protection laws. As Sathyanarayanan argued in another communication to WhatsApp: 'The game plan is very clear, i.e., to transfer the entire existing user base committed to updated 2021 privacy policy before the Personal Data Protection (PDP) Bill becomes the law' ('*Competition Commission of India Suo Moto Case No. 01*', 2021, pp 3–4).

Alongside the evidence presented in this chapter, Karmanya Singh's reflections on the 'balance' that is carefully weighed up by Big Tech in navigating its legal liability indicates how WhatsApp, and Meta, press against and sometimes transgress the boundaries of what is legally permissible in the pursuit of profit. The privacy policy amendments and debate in

legal and public spaces make visible what Alex Jeffrey terms the ‘edge of law’ and how ‘the operation of law is productive of uneven landscapes of power’ (Jeffrey, 2019, p 4). As Cohen argues, Big Tech and the state must necessarily re-work the legal institutions in the face of novel data relations. The ‘notice and consent’ agreement was a fudge by the FTC in the absence of a regulatory framework designed to reckon with practices of data tracking and ‘behavioural advertising’ (Cohen, 2019b, p 56). As the now dominant legal mechanism imposed by US state authority, but shaped by Big Tech’s ambitions, the privacy policy has become a primary legal ‘tactic’ (Jeffrey, 2019, p 22) for engaging the law to legitimize data extraction and enclosure (Cohen, 2019b). Through its privacy policies, WhatsApp redefines the boundaries around what data it collects and processes in ways that exploit the unevenness of data protection laws and discriminates between different users based on the jurisdiction they (and their phone number) inhabit. As WhatsApp’s privacy revisions and legal opposition testify, the edge of what is legally permissible when it comes to data relations and privacy is ambiguous; something that WhatsApp and Meta can (so far) afford to manipulate through the courts and regulatory fines.

WhatsApp’s privacy policies and ensuing legal debate were not only productive of space, but also of time (see Braverman et al, 2014; Valverde, 2014; Jeffrey, 2019). A primary grievance was that WhatsApp had actively exploited a window of opportunity before the implementation of more stringent data protection policies that would likely hinder their data-sharing ambitions. But the temporality of privacy by law was also evident in other ways during legal proceedings and court appearances.

Both WhatsApp, the Government of India and the courts found mutual, though differing, interest in creating legal drag: slowing down the progress of court proceedings through appeals, forestalling, delays and referrals to future legal judgments. For example, the CCI is critical of WhatsApp’s blatant disregard for due process to hamper legal proceedings. It argued that ‘[D]espite clear directions’ WhatsApp failed to submit its response to the CCI’s order (of 19.01.2021) in the manner requested (‘Competition Commission of India *Suo Moto Case No. 01*’, 2021, p 3), while ‘Facebook neither responded to the queries raised by the Commission nor moved any application seeking extension of time to comply with the requisitions made by the Commission’ (‘Competition Commission of India *Suo Moto Case No. 01*’, 2021, p 3). Following the CCI’s extension, instead of providing the requested information, Facebook pleaded that given ‘Facebook and WhatsApp are separate and distinct legal entities’ it should be ‘not be arrayed as a party to these proceedings’ (‘Competition Commission of India *Suo Moto Case No. 01*’, 2021, pp 3–4).

The Commission interpreted the delayed and inadequate response as an act of ‘non-compliance’ and deliberate evasion of its request for

more information about the nature of integration between WhatsApp and Facebook Company Products. ([‘Competition Commission of India Suo Moto Case No. 01’, 2021](#), p 4). The Commission also took issue with the tone of and justification for WhatsApp’s response which refused to engage with due process while claiming to avoid a ‘delay’ in legal proceedings. WhatsApp wrote that ‘requiring companies to sign every submission, responses, pleadings, etc. to be filed before the Hon’ble Commission is a cumbersome obligation and may result in a delay of proceedings before the Hon’ble Commission’ ([‘Competition Commission of India Suo Moto Case No. 01’, 2021](#), p 4). ‘To avoid any such delay’, WhatsApp ‘authorized its legal representatives to act, appear, plead, and file before the Hon’ble Commission on its behalf’ but did not submit its signing of pleadings even when ‘the legal requirement is crystal clear’. Not only did WhatsApp hinder the proceedings, but it also objected to the relevance of the Commission’s scrutiny claiming that its questions were *sub judice* – that is, overlapping with matters currently being considered in other court cases.

WhatsApp and Facebook subsequently appealed the single-judge order which had refused to halt the investigation by the CCI into WhatsApp’s 2021 privacy policy and sharing. WhatsApp’s senior lawyer then requested a delay in the hearing of the appeals until July 2021 in order for the proposed data protection bill to reach Parliament. When the court reconvened in 2022, the bill was still not under review, Harish Salve for WhatsApp told the court that:

We have given an undertaking to the government. Till the Personal Data Protection Bill (PDP) Bill comes, this (privacy policy) will be in freeze. The coercion that you have to opt-out is gone ... If the Parliament and union government is seized of it where is the question of the CCI banging on. (*Hindustan Times*, 31 March 2022)

Meanwhile in the *Karmanya Singh Sareen v Union of India* hearings, similar justification for further delays were made by Solicitor General Tushar Mehta representing the Government of India and agreed with by WhatsApp’s counsel (Kapil Sibal) that requested the court to postpone the hearing to give time for the Digital Data Protection Bill of 2022 to be introduced and by referring to which ‘would solve many of the issues raised by the petitioners’ ([Spandana and D’Souza, 2023](#)). Despite the opposition of Senior Advocate Shyam Divan who represented the petitioners and called for an immediate hearing given that ‘legislative action is uncertain and the Court must direct its immediate attention to the issue’ the bench decided to wait until the Digital Data Protection Bill was reviewed by Parliament ‘to avoid potential contradictions’ ([Spandana and D’Souza, 2023](#)).

Ironically, in earlier hearings concerning the Karmanya case the Delhi High Court (2016) had reasoned that because the right to privacy in the Indian Constitution had been referred to a ‘larger bench of the Supreme Court’ in *Puttaswamy v. Union of India* the right itself could not be a valid ground to grant relief and deferred a more favourable outcome until such a right was enshrined in the law. And yet, when the Supreme Court finally issued its landmark judgment on 24 August 2017 holding that the Indian Constitution guaranteed a fundamental right of privacy to each individual, this did not serve to close the case. Instead, the Puttaswamy judgement initiated new questions about the implications of a right to privacy for data and informational privacy. To answer these the Government of India commissioned a report led by the retired Supreme Court Judge Justice B. N. Srikrishna. This report became the basis for a new Data Protection Bill which stressed its goal to be *the* framework for data regulation in the global south, recognizing the need for personal data protection but not at the expense of India’s economic growth. A balance which could be in part addressed by data localization to ensure Indians’ data stayed in India (Srikrishna, 2018).

The Data Protection bill was then drafted in 2018 and after lengthy debate, delay and revisions, subject to lobbying by Indian Big Tech and Silicon Valley as well as civil society, were enacted as the Digital Personal Data Protection Act, 2023 (DPDPA). In the DPDPA, the requirement for data localization appeared now absent but the Indian state’s authority is disproportionately empowered. In addition to exercising multiple exceptions to the law the state, unlike private companies, can ‘sidestep’ consent where a citizen has already consented to receiving other benefits from the government, granting the state ever bigger data power (Burman, 2023) and, to some degree, ‘un-making digital personal data protection’ (Taraporevala, 2024). But with the DPDPA rules only recently released for consultation the detail has yet to be fully realized and implemented. Meanwhile the Karmanya Singh Sareen case remains pending.

WhatsApp (and the Government of India) constructively navigated the legal ambiguity concerning data protection and privacy rights in India in ways that were productive of space and time. The lack of legal code concerning data protection within the Indian jurisdiction proved opportune for a new version of the privacy policy fiction to be performed. Which, when under scrutiny, could only be challenged by a ‘moving frontier’ of privacy law yet to come (Jeffrey, 2019, p 40). As a beneficiary of big data, through its own digital public infrastructure, the Government of India along with WhatsApp, is in no hurry to delimit the edges of data and privacy rights; to enclose what data can and cannot be collected, shared and processed. Meanwhile, with or without Indian data regulation, citizens’ data rights remain sublimated to the interests of Big Tech and the state.

The privacy game

‘We’re in a competition for people’s trust’

In his book *The Great Tech Game*, [Suri \(2022\)](#) interprets the shifting relations between Big Tech, governments and citizens as a global contest for technological, economic and geopolitical dominance that is shaping the world’s political and economic order. The competition for privacy, trust and authority is certainly a key part of this game. For WhatsApp’s CEO, Will Cathcart, the ‘competition for people’s trust’ was about whether WhatsApp could sell ‘privacy’ better than other digital private messaging apps ([ASPI, 2021](#); [Kantrowitz, 2022](#)). The privacy policy amendments and ensuing litigation raised questions about the Indian state’s capacity to protect both national and individual data ownership and privacy rights and curtail corporate power in India. But the public and legal push back against the privacy policy updates represented a more unusual challenge to WhatsApp’s private authority and legitimacy. Drawing on recent literature, [Srivastava](#) documents that, as private providers of a ‘public good’, Big Tech companies must ‘carefully construct an image of a responsiveness and attentiveness primarily concerned with responding to its user community, much like politicians must do with their constituents’ ([Marichal 2012](#), p 46 cited in [Srivastava, 2021](#), p 994). Equally, if not more important than responding to the formal legal spaces of court hearings, petitions and lawyers, WhatsApp had public privacy work to do in repairing public trust in its product and privacy principles and restoring its legitimacy as a private tech corporation delivering a public utility in India. A few important factors shaped WhatsApp’s response.

First, it sought to reframe the narrative concerning people’s grievances about their policy changes in a more favourable light. It attributed the public response to a series of misunderstandings and confusion promoted by misinformation and, admittedly, its own poor communication about the updates. WhatsApp implied that the problem was not its updated terms, but rather people’s limited grasp of the detail. To combat this, WhatsApp announced that it would be ‘giving more time’ for users to better educate themselves about the privacy policy update by deferring the deadline from 8 February 2021 to 15 May 2021 ([WhatsApp, 2021b](#)). On their blog, WhatsApp said:

We’ve heard from so many people how much confusion there is around our recent update. There’s been a lot of misinformation causing concern and we want to help everyone understand our principles and the facts.

We’re also going to do a lot more to clear up the misinformation around how privacy and security works on WhatsApp. We’ll then go

to people gradually to review the policy at their own pace before new business options are available on May 15. (WhatsApp, 2021b)

In an interview with technology journalist Alex Kantrowitz, Will Cathcart empathized with the people that ‘thought that we’re changing’ to reduce the significance of the update for WhatsApp and frame the moment as ‘a painful reminder of how important it is we communicate really, really clearly about this to the 2 billion plus people who use WhatsApp’ (Kantrowitz, 2022). This line echoed the notice posted on WhatsApp’s webpages which stated: ‘It’s our responsibility to explain these updates clearly’ before setting out that they have ‘provided further clarity about how we collect, share, and use data’. In particular, providing ‘more detail on how we manage your information’ added ‘more detail to certain sections of our Privacy Policy and added new sections’ and ‘also simplified the layout of the Privacy Policy and made it easier for users to navigate’ (WhatsApp, 2021a). Later in its appeal against the CCI’s penalty, WhatsApp argued that ‘[s]uch an extensive review period exceeds industry practice’, for example in comparison with Google’s Terms of Service’ (Meta appeal to CCI 100–101). Ironically, a company well known for its secrecy about the scale of its data collection (Vaidhyanathan, 2012). Second, WhatsApp paid Google to promote its messaging under searches for ‘WhatsApp privacy policy’ and took out full page advertisements in India’s national daily newspapers on 13 January 2021 (Hern, 2021). For instance, on the front page of the *Times of India*, *Indian Express* and *The Hindu*, WhatsApp announced that ‘WhatsApp respects and protects your privacy. Respect for your privacy is coded into our DNA’.

Third, the tone and content of WhatsApp’s response appeared strategic in both its emphasis and omissions. WhatsApp prioritized the message that it protects the ‘privacy and security of your personal chats with family and friends’ and announced that neither WhatsApp nor Meta can see the content of private messages because it is protected by end-to-end encryption, WhatsApp groups remain private, neither WhatsApp nor Facebook can see users’ shared location and WhatsApp does not share user contacts with Facebook or any other app. Concerning what had changed, WhatsApp was more oblique, informing users that when they choose to engage with businesses on WhatsApp ‘these businesses may use Meta as a technology provider to manage some of the responses on their behalf. We will clearly label chats to make you aware when that happens’ (WhatsApp, 2021a). The contexts in which WhatsApp users would engage with businesses over WhatsApp were couched in favourable terms concerning efficiencies and improved customer experience and as something that the user had complete control over: ‘It’s your choice whether you chat with a business on WhatsApp, and you can block or remove them from your contact list’

(WhatsApp, 2021a). In addition to defending the nature of the policy amendments WhatsApp also emphasized its commitment to delivering private messaging infrastructure: ‘We go to great lengths to build WhatsApp in a way that helps people communicate privately.’

Yet, there was no question that the substance of the privacy policy would be altered in response to user or Government of India concerns. WhatsApp’s public narrative came under criticism from internet activists and civil society campaigners who claimed the messaging was both ‘misleading’ by omitting to alert users to the extent and value of the metadata collected by WhatsApp and risked failing in their effort to rebuild public trust. Tripti Jain, a lawyer and researcher with the Internet Democracy Project argued that the ad fails to instil trust in people because

[i]t does not state what data are collected and how [WhatsApp] ... intend to process the data that are collected. They are simply repeating the same things – the app is end-to-end encrypted, private messages are not shared with Facebook. If they really wanted to instil trust in people, they have to explicitly state what they are collecting rather than publishing these deceptive ad. (Ashlin, 2021)

WhatsApp’s initial efforts failed to convince Indian citizens of its intentions; the fallout from the privacy policies continued to occupy the headlines and downloads of Signal and Telegram continued to rise. The Government of India was also not letting up either. In a letter sent on 18 May 2021 from the Ministry of Electronics and Information Technology to the CEO of WhatsApp and published in the media, the minister made clear that WhatsApp’s decision to defer the deadline did not ‘absolve WhatsApp from respecting the values of informational privacy, data security and user choice for Indian users’ (PTI, 2021). But in recent months WhatsApp had been playing another privacy game with the Government of India which was now coming to a head. This game concerned the requirement for ‘traceability’ on private messaging apps and represented another legal platform through which WhatsApp would assert its commitment to citizens’ privacy in India, and globally.

Privacy paternalism and the struggle over authority

Between February and March 2021, a meme circulated on WhatsApp and Twitter that took a frame from the 1967 episode of the Spider-man cartoon series which depicted two spidemen posing opposite each other pointing fingers and accusing the other of being an imposter. Two captions annotated the cartoon with each relating to one of the spidemen, the first says ‘govt taking whatsapp to court because its new privacy policy undermines user

privacy’ and the other states ‘whatsapp taking govt to court because the new IT rules undermine user privacy’.

The meme satirized the growing struggle between WhatsApp and the Government of India over private messaging spaces, privacy and security which had been ongoing since 2018 when concerns arose about misinformation. And hinted at both the government and Big Tech’s paternalistic approach to citizens’ privacy. Just over a month after WhatsApp first announced its privacy policy update, the Government of India published the final draft of The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 on 15 February 2021 (hereafter the Intermediary Rules) ([Government of India, 2021](#)).

The Intermediary Rules sought to provide the government with a legal mechanism to compel ‘significant social media intermediaries’ with at least 50 lakh or 5 million registered users in India ‘to enable the identification of the first originator of the information on its computer resource’ upon issue of a government or court order (Intermediary Rules, 2021, p 2). The legal requirement to trace the person who sent the message on end-to-end encrypted messaging services – also known as ‘traceability’ – would only be for ‘the purposes of prevention, detection, investigation, prosecution or punishment of an offence related to the sovereignty and integrity of India’, this included matters concerning ‘the security of the State’ and ‘friendly relations with foreign States’ as well as ‘public order, or of incitement to an offence relating to the above or in relation with rape, sexually explicit material or child sexual abuse material punishable with imprisonment for a term of not less than five years’ (Intermediary Rules, 2021, p 2).

On the eve of 25 May 2021, the deadline for complying with the guidelines, WhatsApp and Facebook submitted respective petitions in the Delhi High Court suing the Indian government over their new traceability requirements. This was only the second time that WhatsApp had taken a party to court (the first lawsuit was against the NSO Group on 29 October 2019). In setting out its request, WhatsApp emphasized its technical and principled commitment to privacy and security drawing on evidence from its privacy policy, blogs and technical white paper on end-to-end encryption.

It reiterated and further emphasized that since its founding, ‘WhatsApp has built its Services with a set of **strong privacy principles** in mind’ (emphasis added in the petition) (*WhatsApp v The Union of India*, 2021, p 8) and been ‘committed to providing a private and secure space where users can freely communicate without fear of third parties reading or listening to their most private thoughts’ (*WhatsApp v The Union of India*, 2021, p 5). The petition also built its case by drawing upon comments submitted by civil society, human right and business entities (including Mozilla, the

Electronic Frontier Foundation (EFF), and the Center for Democracy and Technology to the Government of India in response its Draft Information Technology (Intermediary Guidelines (Amendment)) Rules, 2018 ('Proposed Amendments') published on 24 December 2018.

WhatsApp's objection to the 'Intermediary Rules' was that 'traceability' violated citizens' fundamental right to privacy which more recently also includes the right to anonymity. The petition argued the case that 'traceability' would inescapably break encryption with implications for WhatsApp's service not only in India, but globally. The creation of 'backdoors' (*WhatsApp v The Union of India*, 2021, p 26) would create 'the capacity for surveillance at will' (*WhatsApp v The Union of India*, 2021, p 28). Moreover, they argued that compelling companies to modify their core infrastructure would undermine trust (*WhatsApp v The Union of India*, 2021, p 28). While current litigation involving WhatsApp and the right to privacy in India had so far failed to successfully mobilize the Puttaswamy judgment to reach a decision, WhatsApp explicitly drew on the conditions set out in *Puttaswamy I* to justify an intrusion into the fundamental right of privacy. It argued that Rule 4(2) of the Intermediary Rules did not meet Puttaswamy's criteria concerning the: (1) legality; (2) necessity; or (3) proportionality of the request.

Concerning the first of these conditions, WhatsApp argued that there was currently no law that would authorize the government to violate citizens' privacy rights to trace the original messenger. Second, Rule(42) did 'not guarantee against arbitrary State action' as government requests for traceability would not be subject to 'judicial oversight let alone prior judicial oversight'. Third, to be proportional, the infringement of fundamental rights must 'be through the least restrictive alternatives', yet to enact traceability would require WhatsApp 'to build the ability to identify the first originator of every communication sent in India on their platforms for all time, infringing upon the privacy of even lawful users' as there is no way to predict which messages will be subject to a court order(s) (*WhatsApp v The Union of India*, 2021, pp 9, 36). Moreover, that WhatsApp was 'designed to facilitate the exchange of private communications' made the harm of ongoing surveillance of all 'private communications' ... 'particularly dangerous and disproportionate as the Impugned Rule does not impose a time limit' (*WhatsApp v The Union of India*, 2021, p 39). This possible new reality would produce a 'chilling effect' on WhatsApp users who rely on the platform for secure and private communications to conduct vital humanitarian work. In proclaiming the Intermediary Rules an 'unconstitutional invasion of the fundamental right to privacy' and 'illegal', the petition also urged the Supreme Court to declare that 'no criminal liability may be imposed for any alleged non-compliance with Impugned Rule 4(2)' (*WhatsApp v The Union of India*, 2021, p 10).

The Government of India responded the next day to state its respect for citizens' right to privacy which would not be intentionally violated on requesting WhatsApp to disclose the origin of a particular message. However, citizens' right to privacy is secondary to 'the responsibility of the government to maintain law and order and ensure national security'. The tone of the press release aimed to reassert the state's authority, calling WhatsApp's petition an 'act of defiance' and expressing disappointment that despite earlier opportunities WhatsApp had not raised the impossibility of traceability. As such, the timing of their petition 'at the very last moment' was interpreted as 'an unfortunate attempt to prevent the [Rules] from coming into effect' (Government of India, 2021).

The competition over privacy had less to do with the substantive rights of India's citizens and their data and far more to do with a struggle over authority, between the state and Big Tech, and their respective legitimacy in the eyes of India's citizen-users. As Aditi Agrawal, tech journalist, suggested in our interview, legal ambiguity concerning digital privacy rights was generative for both WhatsApp and the state's claim to authority and legitimacy. Agrawal said,

On the one hand the Government of India can mobilise its Intermediary Rules to tell the electorate 'See, we care about your privacy and safety online, and therefore we introduced the traceability provision. But look at this evil American company. They challenged it. We can't do anything. We have to wait for the courts.' And on the other hand, WhatsApp can say 'Look, we care about your privacy, which is why we dare to go against the Indian Government. We have literally filed only two cases the worldwide: one was against the NSO Group and one against the Indian Government on the traceability provision. See how much we care about privacy! You should trust us, now it's up to courts.' Both the government and WhatsApp can pass the buck to the courts and claim the higher moral ground when it comes to caring about Indians' privacy. The courts, in the meanwhile, take their merry time to come to a decision, if at all. Four years since the lawsuit began, no headway has been made.

Conclusion

Questions of privacy surface at the legal boundaries and become socialized and animated through privacy policies, court documents and legal proceedings. In this case, amendments to WhatsApp's privacy policies presented ruptures in the company's data-sharing and privacy practices which attracted public and legal critique within India and beyond. We have documented the geography to WhatsApp and Meta's practices as they constructively navigated India's

geolegal ambiguity concerning data protection and privacy and presented the company's un-making of data privacy as simultaneously a non-event and inevitable for the platform's development and improved user experience. Operating at the boundaries of the law, WhatsApp's 'legal entrepreneurialism' in the context of legal and public challenge demonstrated not just how the law is productive of space and time, but how the edges of the law 'are productive of uneven landscapes of power' and to be exploited for profit (Cohen, 2019a; Jeffrey, 2019). This is one aspect of Meta's privacy game and it finds public expression in WhatsApp and the Indian government's struggle over trust, legitimacy and authority as each assert their paternalism with respect to citizen-user privacy. It is also articulated through higher democratic ideals. The government of India perceives WhatsApp's opportunism as an affront to its data sovereignty and there too, democracy while WhatsApp accuses the government of undermining democratic freedoms by calling for 'traceability'.

In a post-colonial context of state surveillance, informational capitalism and data colonialism, citizen-users and activists remain sceptical of Big Tech's privacy promises. Petitions against WhatsApp challenged the fiction of consent, choice and control and the authenticity of WhatsApp's privacy promise. In a bid to attain or maintain its private authority, WhatsApp and Meta strategically reframed the privacy policy problem as a public misunderstanding and deflected attention away from its shifting privacy principles by suing the Government of India for disregarding Indian citizens' privacy rights and demanding 'traceability' on WhatsApp and other messaging platforms. As we explore in the [next chapter](#) WhatsApp's privacy narratives evoked privacy-by-design, notably end-to-end encryption, to elevate and justify its role and responsibility as a global protector of privacy in its appeals to governments and citizen-users alike.

Privacy-by-design

This chapter turns to the design of WhatsApp's privacy architecture, that is the system, software and code through which WhatsApp has been iteratively developed by software engineers in dialogue with intimate geopolitics and privacy questions. [Chapter 5](#) examined how WhatsApp designs and narrates privacy meaning, values and boundaries through its privacy policies, petitions and appeals – to communicate and transform the contours of privacy norms within India, and beyond. There, WhatsApp's response to calls for traceability foregrounded its technical architecture and, in particular, end-to-end encryption to underscore its commitment to privacy and navigate relationships with national governments. This chapter focuses more directly on the materiality of privacy and how it is designed, imagined and narrated by WhatsApp, whereas Indian users' privacy stories are the subject of the [next chapter](#). Where tectonics means 'to build', we're concerned with how privacy is designed and 'built' into digital architectures and how design practices evolve in response to geopolitical and socio-cultural changes (Frew, nd).

In architectural practice, tectonics is about *more than* what is built or the construction alone, it also recognizes the role of 'poetic' and 'interpretive construction' which British architect and critic Kenneth Frampton calls a building's 'tectonic expression' which dialogues with social, political and cultural processes ([Frampton, 2001](#)). We adopt this concern in our approach to privacy-by-design, recognizing its construction as just one aspect of WhatsApp's digital privacy architecture and focusing on the relationship *between* design, materiality, discourse and power and its wider impact. We examine the structure and construction of end-to-end encryption, which as security infrastructure comes to signify a privacy 'thing' which is given expression through 'privacy talk'. This relationship between 'privacy things' and 'privacy talk' concerns how WhatsApp designs *and* communicates its technical, often hidden, privacy architecture to strategically engage users, itself, governments, regulators and policy makers to navigate litigation, build consumer trust and gain competitive advantage.

The growth of Big Tech has given new prominence to software ‘coders’ as the architects designing contemporary society and as the solution to problems. Clive Thompson (2019) argues that software ‘programmers are ... among the most quietly influential people on the planet’ in ‘a world made of software, they’re the architects’ (Thompson, 2019, pp 10, 11). Like architects, coders make decisions about how we, the users, engage with technologies and inhabit digital environments; they can determine how easy or difficult certain actions are or encourage us to do more or less of a particular activity. We can think of code as a technology: as Thompson explains, code is engineering but unlike mechanical, industrial or civil engineering – ‘the machines we make with software are woven from words’ ... ‘Code is speech; speech a human utters to silicon, which makes the machine come to life and do our will’ (Thompson, 2019, p 14). Unlike a machine which does things in situ and in singular form, code is a machine that ‘can be replicated globally for little-to-zero marginal cost of distribution’ (Thompson, 2019, p 309).

Importantly, code can be edited in response to problems, to *improve* how users dwell in and engage with digital spaces. Talking about the issue of misinformation on WhatsApp, Will Cathcart, Head of WhatsApp, compared the work of his software developers to that of architects when he said that ‘sometimes on the team we talk about it as solving the problem as an architect would rather than as a law enforcement officer would’. This is important because ‘architects think a lot about the design of a building, the design of a city, what can you do that will help create a safe or safer environment over time’. Cathcart went on to emphasize that ‘the private nature of the product’ in particular the presence of encrypted messaging ‘has pushed us more towards architect type solutions’ in how we shape people’s behaviour and their experiences with the app (Vox Media Podcast Network, 2022).

WhatsApp’s founders were attentive to the fact that ‘the decisions they make guide our behaviour’ (Thompson, 2019, p 11). One of Koum and Acton’s fundamental design principles for WhatsApp was to make messaging ‘simple’. This ambition was translated into the technical architecture which ensured that users encountered minimal obstacles to accessing the app, for instance only requiring users to share a phone number, reducing friction on the app by banning pop-up advertisements and massively cutting the cost of sending messages on mobile by working over the top of existing data plans and internet. Such intentional design features made WhatsApp a simple space through which to share information and communicate with their contacts multiple times a day. The automatic addition of a user’s address book to WhatsApp’s contacts and the potential to create WhatsApp groups further facilitated the ease and speed with which information could be circulated and at scale.

This chapter therefore builds on decades of knowledge produced in science and technology studies, philosophy of technology and feminist

technoscience that contends that technology and design are not neutral practices. Technology is political, it is produced within situated sociopolitical constellations and potentially transforms them too (Winner, 1988). Feminist technoscience and carceral technoscience have highlighted the partial and situated design of technology that is inherently discriminatory along lines of gender and race. As Wajcman argues: ‘[a] range of social factors affect which of the technical options are selected. These choices shape technologies and, thereby, their social implications. In this way, technology is a sociotechnical product, patterned by the conditions of its creation and use’ and in turn revealing of ‘continuities of power and exclusion, albeit in new forms’ (Wajcman, 2004, pp 34, 54, see also Benjamin, 2019). Privacy architecture is politics. WhatsApp’s technical decisions and designs for users’ privacy should be understood as political decisions, that carry meaning and power and coproduce intimate geopolitical life.

Drawing on his experience in digitizing government processes, Richard Pope (2016) reasons that ‘if politics is about this distribution of power in society, software is now politics. The decisions of designers and developers are a political force of their own. And we are asking users to trust us with more data, to allow code to make more decisions for them all the time’ (Pope, 2016). Software programmers do not only determine the instructions that constitute the code, but they also make decisions about what product is designed, what problems get solved and what even constitutes a problem in the first place. Who are the software programmers in Silicon Valley? Though writing in 2004, it remains the case that when it comes to Big Tech ‘the culture of computing is predominantly the culture of the white American male’ (Wajcman, 2004, p 112). What are the implications of that dominant culture for imagining and designing privacy architecture?

Finally, in recognizing the inherently political nature of all technologies, however ordinary and banal and that mediate so much of our everyday lives, we make a case for examining the (geo)political life of privacy-by-design. Privacy-by-design is the industry gold standard (since 2010) first advanced by Ann Cavoukian, the Privacy Commissioner of Ontario, Canada in the 1990s and notably in the context of the 32nd International Conference of Data Protection and Privacy Commissioners. Privacy-by-design is grounded in ‘a growing understanding that innovation, creativity and competitiveness must be approached from a “design-thinking” perspective – namely, a way of viewing the world and overcoming constraints that is at once holistic, interdisciplinary, integrative, innovative, and inspiring’ (Cavoukian, 2010). This works from the principle that privacy cannot be guaranteed by adhering to regulatory frameworks alone and must be embedded into networked data systems and technologies, organizational priorities, project objectives, design processes and planning operations. ‘Privacy must be embedded into every standard, protocol and process that touches our lives’ (Cavoukian, 2010). For,

as Hoepman explains: within our contemporary digital world, ‘relying on the law, the market, or simply the good intentions of people is not enough’ (Hoepman, 2021, p 60), to protect the privacy or security interests of users, society, nations and democratic life.

In our digital age there is also a commercial value to embedding privacy designs within digital architecture where ‘consumers are increasingly aware of their data privacy rights’ and consider a ‘company’s privacy standards when choosing a product or service’. Therefore, as Nanda argues: ‘[i]mplementing privacy by design can assist businesses not only in achieving efficient compliance with the personal data protection law but also in fostering consumer trust and becoming a competitive advantage’ (Nanda, 2024). This is consistent with Arturo Escobar’s (2017) argument that most design, whether of consumer goods or digital technologies, architecture or policy, ultimately serves capitalist ends. We’re interested in how privacy ‘design’ is a ‘situated and interactive practice’ (Escobar, 2017, p 40). After all,

digital products also live in the social world and change it. Digital design cannot operate outside of its social context, because files, systems and media only gain meaning as part of a community’s practice. Effective, meaningful design is a social activity, in which the design is one actor among many. (Kommonen, nd cited in Escobar, 2017, p 41)

The (geo)politics of end-to-end encryption

Privacy was not always central to WhatsApp’s objectives and brand identity, at least not quite so explicitly as it is today. When Koum and Acton initially set out to develop WhatsApp, designing privacy features into the app’s architecture was not a key priority. Taking a journey through the Internet Archive of WhatsApp’s ‘home page’ reveals how WhatsApp’s brand identity has evolved (Santos and Faure, 2018). Acton and Koum’s first priority was to create a fast, reliable and inexpensive messaging system that ‘allows you to carry on a conversation in real time with your mobile contacts without having to pay for SMS’ and where ‘iPhone users can also enjoy unlimited MMS features that let you share images, video and audio media.’ (WhatsApp, 2010). It was to be ‘Fast. Personal. Awesome’ (WhatsApp, 2011). As the capacity to connect across platforms and create groups materialized, that narrative shifted to ‘Awesome. Cross platform. Now with group chat’ (WhatsApp, 2011). By 2012 the technical and personable nature of the platform found expression in ‘Simple. Personal. Real time messaging’ (WhatsApp, 2011). Koum and Acton elucidated their personal commitment to WhatsApp’s simplicity by emphasizing their antipathy towards advertisements which demanded intensive data mining and processing and ultimately diminished

the user experience. As we explained in [Chapter 1](#), WhatsApp's founders were adamant that advertisements not only disrupted the aesthetics and flow of a product but were also labour intensive given the work needed to mine, clean and process data. This all detracted from the time that could be spent developing an affordable, reliable messaging app.

Koum and Acton's minimal approach to user data was arguably more influenced by their distaste for business models driven by advertisements rather than a commitment to prioritizing users' data privacy. 'Simple. Personal. Real time messaging' remained a consistent strap line from 2012 until 2016. But that changed in 2016 with the appearance of a new slogan: 'Simple. Secure. Reliable messaging'. This subtle shift in wording signalled a new commitment to data security and a transformation in WhatsApp's relationship to users' data and its relationship to Facebook.

The introduction of end-to-end encrypted messages by default coincided with the integration of WhatsApp and Facebook's technical infrastructure and a new emphasis on the 'private' nature of communication on the platform. Writing in their blog, Acton and Koum explained the new security development:

we're proud to announce that we've completed a technological development that makes WhatsApp a leader in protecting your private communication: full end-to-end encryption. From now on when you and your contacts use the latest version of the app, every call you make, and every message, photo, video, file, and voice message you send, is end-to-end encrypted by default, including group chats. ([WhatsApp, 2016a](#))

Koum and Acton had begun work on end-to-end encryption in summer 2013 before the deal with Facebook was finalized. At the time, encryption was in its relative infancy, typically the preserve of cryptoactivists and cryptographers like Moxie Marlinspike whom Brian Acton met in late 2013. Marlinspike had recently left Twitter and a million dollars in stock to start a collaborative project called Open Whisper Systems focused on developing open-source versions of the encrypted texting programme (Text Secure) and encrypted voice calling app (RedPhone). By 2014 Open Whisper Systems had merged Redphone and TextSecure into a single encryption communication tool for Android and iOS called Signal ([Wiener, 2020](#)). Reportedly impressed by Marlinspike's character and the potential of encryption, Acton worked with Marlinspike to implement the Signal protocol in WhatsApp and create an end-to-end encrypted messaging architecture.

Encryption is a form of cryptography which is 'the art of creating and using methods of disguising messages, using codes, ciphers, and other methods, so that only certain people can see the real message' ([Froomkin, 1995](#), p 713).

Encryption is important for the security of the original digital message – the plaintext – which must pass through WhatsApp’s data servers and always remain protected from potentially interested parties whether that’s technology or telecommunications companies or governments or criminals. The form of encryption used by WhatsApp is called end-to-end which refers to a method where the plaintext leaving a phone or laptop, let’s call this Alice’s device, as is the western convention for explaining cryptography, is scrambled using a mathematical algorithm into a ciphertext which is gibberish and difficult to decode (Froomkin, 1995). The algorithm for creating the ciphertext is accessed by Alice’s device using the ‘public key’ on Bob’s device *before* sending the message to the server. The ciphertext is stored on the server until Bob is ready to receive it at which point the corresponding ‘private key’ on Bob’s phone decrypts the ciphertext into plaintext. This means that only Alice, the sender, and Bob, the recipient, have access to the plaintext. At all other stages, the message exists as indecipherable ciphertext. Hoepman points out that until 2017 messages were only encrypted between Alice’s device and Facebook’s server and between Facebook’s server and Bob’s device meaning they were available as plaintext while waiting to be delivered on the Facebook server. ‘This is clearly undesirable as it would allow the messaging service provider ... to scan the messages and use their content to target WhatsApp users. (In fact, this was for a long time how WhatsApp worked, until 2017, but Facebook claims it never abused its potential to access these plaintext messages)’ (Hoepman, 2021, p 82).

The implementation of end-to-end encryption by default on WhatsApp for its billion plus users was unprecedented. This move transformed encryption technology from a fringe technology for security and privacy specialists into a mainstream technology that would, in time, acquire a new kind of name recognition (Burgess, 2023). But what was the value of introducing encrypted messaging by default at this particular moment? After all, as Santos and Faure question, since very few users would ever ‘see’ the effects of an otherwise invisible or seemingly immaterial software code what benefits would encryption bring to WhatsApp (Santos and Faure, 2018)? As we outline here by building on their argument, the initial rationale for encryption extended beyond the interests of users’ data security to include both personal as well as geopolitical dimensions.

The implementation of end-to-end encryption was reportedly personal. Although not averse to the introduction of encryption, Mark Zuckerberg and Sheryl Sandberg had queried the financial implications of placing personal messages out of the company’s reach when Acton and Koum shared their plans in 2014 (Levy, 2020), given the boundaries this would place around the potential to monetize activity on the app. By 2016, work to integrate Facebook and WhatsApp’s technical infrastructure was complete and the new privacy policy updated users’ consent for data to be shared between

WhatsApp and Facebook for the first time. Around the time that WhatsApp announced the expansion of its data-sharing practices with Facebook, Koum and Acton also blogged about the implementation of end-to-end encryption by default. On the one hand, the privacy threshold of users' metadata was lowered, given greater sharing across the platforms but on the other hand, the security of personal communications was enhanced through encryption.

Neeraj Arora, who joined WhatsApp as their Chief Business Officer in 2011 and made the move to Facebook with Acton and Koum, has argued that introducing encryption at this point served a more clandestine objective for WhatsApp's founders. Speaking in a media interview, Arora commented that: 'Obviously Jan and Brian might never put this on the record that we were doing this [building end-to-end encryption] partially so that Facebook never gets any information about our users, but I know for sure that was one of the reasons they wanted to do it' ([Vox Media Podcast Network, 2022](#)). Arora's admission signifies how a technical affordance was, in part, a personal political move by WhatsApp's founders that was intended to frustrate Facebook's classic playbook and Zuckerberg's ambition to monetize WhatsApp by extracting value from user's personal messages.

The launch of end-to-end encryption also carried geopolitical power for WhatsApp, especially in its biggest markets in the global south where it was encountering criticism, if not hostility from some governments. Santos and Faure argue that encryption as software was 'a form of power carried out by its developers' that responded to emergent political and legal dilemmas faced by WhatsApp in Brazil ([2018](#), p 12). In 2015, Judge Sandra Marques in Sao Bernardo do Campo, Sao Paulo imposed a ban on WhatsApp for failing to respond to two notifications (in July and August) to hand over personal messages exchanged between individuals subject to a criminal investigation, leading the prosecutors to request the ban. Mark Zuckerberg criticized the court order in a Facebook post: 'This is a sad day for Brazil. Until today, Brazil has been an ally in creating an open internet. Brazilians have always been among the most passionate in sharing their voice online.' And expressed his moral outrage that the work of Facebook to protect users' data could be undermined by the decision of a judge: 'I am stunned that our efforts to protect people's data would result in such an extreme decision by a single judge to punish every person in Brazil who uses WhatsApp' ([Zuckerberg, 2015b](#)).

The decision was over-ruled by a higher court judge 24 hours later who contended that: 'It has not been shown reasonable that millions of users should be affected as a result of the company's inertia', this was not before 1.5 million users had downloaded Telegram in search of an alternative OTT messaging app ([Philips, 2015](#)). In March 2016 Diego Dzodan, a Facebook executive was arrested for again failing to 'cooperate with an investigation into drug trafficking and organized crime' ([AP, 2016](#)). By May 2016 when a further ban was imposed for 72 hours by a judge frustrated by Facebook's

lack of compliance, Facebook could argue that WhatsApp had no power to access the data being requested due to its encrypted state (Slay, 2016). In a Facebook post (no longer available) Koum wrote:

Yet again millions of innocent Brazilians are being punished because a court wants WhatsApp to turn over information we repeatedly said we don't have. Not only do we encrypt messages end-to-end on WhatsApp to keep people's information safe and secure, we also don't keep your chat history on our servers. When you send an end-to-end encrypted message, no one else can read it – not even us. (cited in Slay 2016)

In a geolegal context where users' privacy rights are more vulnerable in the face of a strong state, Santos and Faure (2018) contend that WhatsApp deliberately mobilized end-to-end encryption as a 'techno-political statement' that allowed them to position themselves on the side of the user vis-à-vis a populist, if not authoritarian government as maintaining individual's privacy. And, as a para-legal weapon, end-to-end encryption acted as WhatsApp's technical foil to the Brazilian government's coercive demands to 'collaborate' on security matters.

Code power, privacy power

This argument proves extremely productive for interpreting the geopolitical and legal encounters between WhatsApp and the Indian government over matters of national security and users' privacy and the expressive power of software code within digital geopolitics. As we introduced in Chapters 2 and 4, the Government of India attributed incidents of violence in 2017 and 2018 to the circulation of misinformation on WhatsApp. Arguing that societal violence was the product of this newly popularized digital technology, the Government of India held WhatsApp accountable and pursued the company to 'trace' the first originator of the messages responsible for inciting violence. Chapter 5 explained how these incidents were, in part, what prompted the Government of India to release its draft Information Technology (Intermediary Guidelines and Digital Media Ethics Code) (Amendment) Rules in December 2018, setting out these proposals, and which were subsequently finalized and published in 2021.

WhatsApp rejected the government's techno-determinist interpretation concerning misinformation on its platform and violence and insisted that the issue be located within society and the state as well. Reluctant to be drawn into India's domestic politics, WhatsApp argued that the guidelines and their insistence on traceability would compromise the 'private nature of WhatsApp'. Carl Woog, a spokesperson for WhatsApp, made this case that: 'People rely on WhatsApp for all kinds of sensitive conversations,

including with their doctors, banks and families. Building traceability would undermine end-to-end encryption and the private nature of WhatsApp, creating the potential for serious misuse' ([Tech Desk, 2018](#)).

The relationship between end-to-end encryption and user's privacy was reiterated by Chris Daniels, then WhatsApp Vice President, when he visited India in October 2018. Although mainly focused on exploring how WhatsApp could help Indian businesses and drive economic growth, attention returned to the need to trace messages and messengers on WhatsApp, but as Daniels explained: 'To do this, we would have to redesign our systems and revise our privacy standards to indiscriminately track user data. We think this is overly intrusive from a privacy perspective' ([Anonymous, 2018](#)).

Moreover, in both the Brazilian and Indian cases, WhatsApp draws on encryption to position itself on the side of citizens and vis-à-vis their national governments ([Santos and Faure, 2018](#)). In the context of the backlash to the 2021 privacy policy update and the implementation of the Intermediary Rules outlined in [Chapter 5](#), WhatsApp moved to sue the Indian government for undermining Indian citizens' right to privacy. In its petition, WhatsApp's lawyers presented the demands to 'break' encryption as a direct challenge to Indian citizens' fundamental right to privacy and freedom of speech:

the requirement that intermediaries like Petitioner enable the identification of the first originator of information in India on their **platforms puts end-to-end encryption and its benefits at risk**. There is no way to predict which message will be the subject of such a tracing order. Therefore, Petitioner would be forced to build the ability to identify the first originator for *every* message sent in India on its platform upon request by the government forever. This breaks end-to-end encryption and the privacy principles underlying it, and impermissibly infringes upon users' fundamental rights to privacy and freedom of speech. ('[WhatsApp LLC v Union of India \(Special Leave Petition\)](#)', 2021, p 6, emphasis in the original)

With end-to-end encryption, users feel safe to communicate freely. However ... enabling the identification of the first originator of information in India on WhatsApp breaks end-to-end encryption and infringes user privacy. As a result, it also significantly restricts the right to freedom of speech and expression online. Once citizens become aware that SSMLs have built the ability to identify the first originator of information in India on their end-to-end encrypted messaging services, individuals will not feel safe to speak freely for fear that their lawful private communications will be used against them, thereby infringing their rights to privacy and free speech. ('[WhatsApp LLC v Union of India \(Special Leave Petition\)](#)', 2021, p 44)

In the months following the company's submission to the High Court of Delhi, Will Cathcart participated in a series of media interviews to promote WhatsApp's commitment to privacy within the wider public sphere. Speaking to the *New York Times*, Will Cathcart explained that:

It's why we fought so hard to bring end-to-end encryption all around the world, and defend it all around the world, at times, with scepticism from governments, or people who are opposed to that level of security saying, 'Well, do people really care about privacy of this stuff?' Yes, people absolutely care about the privacy of this stuff. (Kantrowitz, 2022)

In another interview, Will Cathcart projected that in ten years

There will be even more sophisticated hackers, spyware companies, hostile governments, criminals trying to get access to it. And not having the best security means that information is stolen. I think that has real consequences for free society ... My hope is that over the next few years, increasingly governments will realise that on balance, the more important thing for them to do is protect their citizens' data. (New York Times, 2021)

WhatsApp's corporate storyline has repeatedly narrated the immateriality of encryption's code as a non-human actor that fundamentally limits the very possibility of responding to the Indian government's request to trace messages and their original messenger on their app. Writing about 'code/space' and the implication of software in our everyday lives, Kitchin et al argue that software and code are 'made to do work in the wider world' and that power is not intrinsic to it, but 'arises out of interrelationships and interactions' with the world (Kitchin and Dodge, 2011, pp 39, 40). WhatsApp therefore affords encryption a form of 'code power' when it mobilizes encryption code as a non-human actor in geopolitical spaces of tech diplomacy in ways that ultimately challenge national sovereignty and effect the relationship between Big Tech and governments.

In their interview rounds and legal documents, WhatsApp's heads and lawyers have willingly exercised a degree of slippage in how encryption as security infrastructure is equated with citizens' privacy and the 'private nature of WhatsApp'. But encryption and privacy are not the same thing. As Waldman points out, as a form of data security, encryption is a constitutive part of digital privacy. '[E]ven for those who think privacy is and always will be about choice and control, it is clear that privacy is not the same as security or encryption' (Waldman, 2021, pp 84–85). And yet, WhatsApp consistently mobilizes end-to-end encryption as an expression of code power and, thereto, privacy power that supersedes human agency, to push

back against governments who they accuse of inserting a ‘spy clause’ in their internet regulations and undermining citizens’ right to privacy.

The move to sue the government of India should be interpreted within a global context and as a signal to other governments seeking to challenge the integrity of end-to-end encryption. US Attorney General William P. Barr has long fought to allow lawful access to encrypted communications; in 2018 the Australian government passed an encryption bill that would co-opt technology and communications companies into building functionality that enables the government to collect communications data, while the UK’s Online Safety Bill strengthens powers for Ofcom to demand encrypted messenger apps scan users’ messages in suspect cases of child sexual exploitation and abuse and terrorism (Karp, 2018; New York Times, 2021; McCallum, 2022). WhatsApp deploys encryption’s code power to portray itself as the global protector of privacy and democratic values on behalf of citizens everywhere. But as encryption code has no palpable or perceivable impact on the everyday lives of its users, they can’t ‘see it’ or ‘feel it’, we now examine how WhatsApp/Facebook has endeavoured to domesticate end-to-end encryption, especially within India, in ways that attempt to imbue it with meaning and materiality that substantiates WhatsApp’s role as global protector of privacy.

Domesticating encryption

The value of implementing encryption to build consumer trust could only be realized by rendering the technical infrastructure into a privacy ‘thing’ that could be perceived by WhatsApp users. This dilemma has been an increasingly central aspect of WhatsApp’s brand campaigns as it seeks to position itself as a global protector of privacy and compete with other Big Tech over the provision and protection of digital private spaces. Given the technical and invisible nature of encryption technology, WhatsApp has had to work at domesticating end-to-end encryption to make it meaningful to ordinary citizens and grant it commercial value. This has required simultaneously justifying the significance of encrypted messaging and communicating its function so that users adopt, trust and normalize a relatively novel technology within their everyday lives. We document how WhatsApp has utilized metaphors and media campaigns to, first, translate encryption infrastructure into everyday settings that make it perceptible and knowable and, second, transduce encryption technology into a ‘feeling’ of digital privacy that can be experienced and valued.

We are particularly interested in the relationship between technical systems and how privacy is imagined, narrated and performed by WhatsApp. In Chapter 7, we do more to examine these relationships with situated experiences of privacy by ordinary citizens. First, we turn to how encryption

is made perceptible and knowable. It has long been recognized that digital technologies are complex to communicate to general audiences. The emergence of mass-market personal computing in the late 1970s generated a proliferation of metaphors that mediate our comprehension and interactions. To compensate for the fact that ‘we do not speak machine language. Metaphor provides us with the means to understand our complex digital devices’ (Saffer, 2005, p 3). We translate digital technologies and processes into analogue experiences that we are familiar with, ‘we conceptualize one domain in terms of the other’ (Lakoff, 1993). As Hutchins writes:

As the levels of complexity are layered one atop the other in order to produce the high-level behaviors that are the actions we recognize while interacting with the computer, the possibility of talking or thinking literally about the computer’s behavior vanishes. We deal with this complexity and this plasticity by speaking metaphorically about the computer. (1989 cited in Saffer, 2005, p 3)

We have become accustomed to associating the ‘envelope’ icon with sending an email, to ‘storing’ ‘files’ within ‘folders’ on the ‘cloud’ and disposing of unwanted files and folders with a ‘click’ of the ‘mouse’ on the ‘trash can/dust bin’ icon. As cognitive aids, metaphors are powerful linguistic devices for how we navigate and speak about the ‘digital world’, another metaphor. In particular, ‘spatial metaphors ... help visualize what are, effectively, no more than abstract flows of electronic signals, coded as information, representation and exchange’ (Graham, 1998, p 166). As Shaw has argued, ‘You don’t see something until you have the right metaphor to let you perceive it’ (Robert Shaw cited in Saffer, 2005, p 13). Yet, analogue priors do not exist for all digital innovations, at least not in ways that are always technically and legally relevant or accurate. The suggestion that there is a ‘right’ metaphor implies the possibility of universal ways of knowing, which feminist technoscience has constructively critiqued by emphasizing and, moreover valuing, the situated, partial and particular nature of all knowledge (Haraway, 1988). So while metaphors can orientate digital design interactions, they can obscure infrastructures and relationships of power, often in their claims to universality. As ways of seeing ‘[m]etaphors are tools and tropes’ (Haraway, 2004, p 240) and the ‘power is about whose metaphor brings worlds together’ (Star, 1991, p 52 cited in Haraway, 2004, p 240).

The product designers, software engineers and leaders at WhatsApp and Facebook determine the metaphors that *they* believe most effectively communicate what encryption does and its relationship to *their* perceptions of what privacy means. The central motif of Facebook’s 2019 privacy pivot was articulated in terms of a shift away from the public sphere of the digital ‘town square’ to the private realm of the digital ‘living room’ as Zuckerberg

explained: ‘Over the last 15 years, Facebook and Instagram have helped people connect with friends, communities, and interests in the digital equivalent of a town square. But people increasingly also want to connect privately in the digital equivalent of the living room.’ Moreover, privacy matters because it ‘gives people the freedom to be themselves and connect more naturally, which is why we build social networks’. By evoking the idea of the ‘living room’ and private digital messaging as the ‘future of the internet’ it is portrayed as both a familiar and an inevitable feature of Facebook’s and the internet’s progress in understanding and facilitating how people want to and *need* to communicate in more ‘natural’ ways, online.

The spatial metaphor of the ‘digital living room’ is reinforced by the metaphorical imaginary of the ‘padlocked’ encrypted message with its unique ‘keys’. As a form of ‘container metaphor’, the living room signifies a bounded space over which individuals have equal control concerning who can and cannot enter that room (Lakoff and Johnson, 1980, p 29). Where ‘spatial metaphors are rooted in physical and cultural experience ... a metaphor can serve as a vehicle for understanding a concept only by virtue of its experiential basis’ (Lakoff and Johnson, 1980, p 18). Mobilizing the container metaphor of a room located within a home is consistent with one of the metaphors typically applied to conceptualizations of encryption where the room (or other contained space such as a car) is defined as bounded in a space that can be locked with a key and placed out of the reach of third-party surveillance (Froomkin, 1995). Indeed, ‘the metaphor of locked containers arguably remains the dominant narrative in public and political discourse’ in the American context within which WhatsApp’s product designers are inevitably trained and located (Gill, 2018, pp 467–468).

Informing the analogy of the ‘digital living room’ is the assumption that the ‘living room’ and by extension the home is a space of security, trust and familiarity in and through which people can come together, converse and nurture feelings of belonging. This idealized spatial imaginary rests on an assumed universal characteristic of the ‘living room’, yet, it is imagined from somewhere, in this case, *from* Menlo Park, California. As feminist geographers and anthropologists have observed, the home can be a space of oppression rather than nurture; ‘the home is an ambiguously experienced “space of belonging and alienation, intimacy and violence, desire and fear”’ (Blunt and Varley, 2004, p 3, cited in Baxter and Brickell, 2014, p 136). Similarly, digital living rooms can be sites of home making and unmaking (Baxter and Brickell, 2014), that include and exclude, and engender intimacy and alienation. As perceived sites of stability homes can function to obscure the fields of power within which people dwell (Carsten, 2004; Ingold, 2005). Analogizing WhatsApp to the private spaces of the home serves as a powerful metaphor via which Meta can articulate the platform’s privacy pivot. But, as we argue further in Chapter 7, this western, universal idea of the ‘digital

living room’ is situated within diverse and contradictory ways within the Indian context.

Feeling privacy, performing privacy

Accompanying the metaphor of a domestic environment and its analogies to intimate relationships and behaviours, WhatsApp and Facebook/Meta more generally have actively cultivated the *feeling* of digital privacy among users on its platform. As Zuckerberg explains:

There is an opportunity to build a platform that focuses on all of the ways people want to interact privately. This sense of privacy and intimacy is not just about technical features – it is designed deeply into the feel of the service overall. In WhatsApp, for example, our team is obsessed with creating an intimate environment in every aspect of the product. (Meta Developers, 2019)

To be successful brands need to sell emotions, not just products. As Ami Vora, ex-Vice President of Product and Design (2018–2022) at WhatsApp writes in her Substack: ‘When I’m building a product, I think a lot about what it should feel like. What’s the best analogy or metaphor I can come up with to describe that feeling?’ ... ‘For WhatsApp, the central product metaphor I think about is “face-to-face” communication with people you know, reflecting how you’d normally have a conversation in the physical world’ (Vora, 2022).

In a Facebook December 2020 ‘Brand Foundations’ marketing document that was acquired by ProPublica, the company’s emphasis was reportedly on promoting WhatsApp as a ‘paragon of privacy’ through “an emotional articulation” of WhatsApp’s benefits, “an inspirational toolkit that helps us tell our story”, and a “brand purpose to champion the deep human connection that leads to progress”. Moreover, the marketing deck identified ‘a feeling of “closeness” as WhatsApp’s “ownable emotional territory”, saying the app delivers “the closest thing to an in-person conversation”’ (Elkind, Gillum and Silverman, 2021). As well as stressing the role of emotions as a key toolkit for selling privacy, the extracts remind us of how WhatsApp’s fortunes are entangled with Facebook’s.

In the year after, WhatsApp’s first media campaign was launched. In collaboration with Bollywood director Gauri Shinde and advertising house BBDO India, they created a series of short (60-second) stories about how people communicate daily on the app in India. Entitled ‘It’s between you’ or in Hindi ‘*Apna sa lagta hai apno ke beech*’ (translating to ‘one feels at home among one’s own’), the films were translated into seven regional Indian languages and designed to portray tender and poignant moments in people’s everyday lives

that are enabled through the intimate and immediate relationships facilitated by WhatsApp. The film plots only ever allude to the content exchanged over WhatsApp, which are kept hidden from the viewer. The private messages form a subterranean storyline. In ‘Cut it Out’ two sisters communicate over the decision for one of them to get a radical new haircut and in ‘Caregiver’ an older lady learns to live independently following the death of her spouse with the help of a caregiver over WhatsApp.

In a series of Indian media and industry interviews, Avinash Pant, then Director of Facebook marketing (2020–2023), explained the rationale behind the advertisements. ‘We wanted to tell real stories about how people use WhatsApp to have intimate conversations. The endeavour is to highlight that the privacy that WhatsApp provides through end-to-end encryption is not just a feature, but a feeling that leads to real human connections.’ When asked why the focus on privacy, he reiterated the repeatedly cited corporate line: ‘Respect for our users’ privacy is coded into our DNA’, and in addition, ‘we remain committed to helping connect the world privately and protect personal communication in India and all over the world’. Privacy is interpreted as something that when ‘deeply felt, relationships feel more intimate and real ...’ (cited in [Yadav, 2020](#)).

In another interview, Pant reinforced the importance of privacy because

We communicate in different ways with different people, and that is the very essence of our personal connections. What you say and the ability to be yourself comes from the assurance of privacy. With WhatsApp’s end-to-end encryption, we come closest to replicating real-life interactions and that’s when we can truly be ourselves. (cited in [Chaturvedi, 2020](#))

That ‘feeling’ of privacy and potential to ‘truly be ourselves’ was even more expressly communicated in WhatsApp’s next campaign launched in August, 2021. In the aftermath of the backlash to WhatsApp’s privacy policy update WhatsApp doubled down on its privacy features, placing it at the centre of its marketing campaigns ([Elkind, Gillum and Silverman, 2021](#)).

The campaign called #MessagePrivately, again in collaboration with advertising agency BBDO India, sought to embed and vernacularize WhatsApp’s effect and affect in people’s everyday lives. One ad shown in India called ‘the Golden Jubilee’ featured an urban middle-upper-class/caste elderly couple celebrating their wedding anniversary in the company of their grandchildren. The grandchildren ask the grandfather to kiss the grandmother but he declines and instead moves to sit in another corner of the room. He then sends a WhatsApp message to the grandmother who smiles to herself, then looks across to her husband and in jest raises her hand in a slap action, insinuating that he has sent her something risqué via

WhatsApp. Neither we, the audience nor the grandchildren see the message sent, reinforcing WhatsApp's message that privacy is embedded in their product ethos and design. In the Indian context, where public displays of affection are usually seen as inappropriate even among married couples when surrounded by family, WhatsApp positions itself as the natural extension of sociodigital intimacy. This particular ad illuminates the additional degrees of privacy that WhatsApp provides even *within* the 'real' context of a family celebration and domestic setting.

Speaking some months after WhatsApp's 2021 privacy policy update Will Cathcart attempted to reassure users that their personal communications were not being shared with Facebook or third parties. He defended WhatsApp's commitment to protect encryption and privacy in the face of governments' requests to share messages in the name of national security. In an interview with technology publication *The Verge*, Cathcart's storytelling operated to historicize (digital) privacy as something that has always been intrinsic to the human experience, as he explained:

one thing I find helpful is thinking through real-world analogs. A lot of stuff feels so new that the debates feel very new, but the real-world equivalents, they're not new. People have been able to meet in private in person and talk privately for hundreds and hundreds of years, and there's no automatic system keeping a backup. There's no automatic system relaying it to a company. And I think that's been a good thing.

Like Vora, Will Cathcart recognized the value of emphasizing and mobilizing the emotional aspects of privacy, as he continued to articulate his, and WhatsApp's privacy imaginary:

Sometimes when you look at some of the proposals on breaking encryption, or traceability in India, or scanning every private photo against the database, and you just apply it to 'Hey, how would you feel about doing this in people's living rooms?' Most people have an instinctive horrified reaction. I think that's telling. (cited in [Newton, 2021](#), np)

It is important to pause and consider exactly how WhatsApp and the stories it tells us, the users, are aimed at constructing its privacy-friendly brand; determining what privacy is, how it feels and what kind of experiences or data its users should be most concerned about. We argue that WhatsApp engages metaphors to create a particular and arguably partial context for imagining what privacy means. Equating privacy with a feeling or spatializing and historicizing privacy, constructs a particular context within which we are encouraged to feel 'alarmed' when privacy is violated by third parties.

Neil Richards, an expert on privacy law, characterizes this kind of thinking about privacy, as the intrusion of someone into a private space, as the ‘creepy myth’; ‘a seductive trap’ that is ‘socially contingent and highly malleable’ (Richards, 2022, p 82) and ultimately serves to conceal the power behind (re)producing privacy. Richards argues that ‘The creepy trap tricks us into thinking that privacy is about psychology, subjective preferences, and consumer empowerment, when privacy is really about money, power, and the ways in which human information rules are used to manipulate consumers and citizens alike’ (Richards, 2022, p 87).

Just as the designers of Facebook’s technical architecture and algorithms transformed social norms concerning the publicity of personal information and relationships, we argue that WhatsApp (and Meta) is seeking to shape norms concerning digital privacy in ways that also align with its commercial interests. ‘Thinking of privacy in terms of creepiness is not only a bad way of gauging whether there’s a real privacy issue; it also confuses us about what’s really at stake, and it further enables the exercise of power by those who control our data’ (Richards, 2022, p 87). By centring the feelings and imaginaries of privacy afforded by end-to-end encryption, which protects against the intrusion of *other* third parties, be they ‘hackers, criminals or rogue governments’, WhatsApp enacts a double manoeuvre. First, it reinforces its authority and reputation as the global protector of privacy, fighting to secure the content of users’ personal messages against rogue actors including governments. And second, it deflects attention away from the *other* routine forms of privacy incursions enacted when WhatsApp (automatically) collects information about its users and their behaviour, their metadata.

Privacy as deflection and the importance of metadata

What is metadata and why should it matter to WhatsApp’s users? In the US, where WhatsApp was founded, the communications law draws a distinction between ‘content’ and ‘metadata’. Metadata can be thought of as the technical data, the context to personal messages which is accessible to WhatsApp in contrast to the content of personal messages which is encrypted. Typically, metadata has not been subject to the same kind of regulation as the content of messages ‘[b]ecause of its technical nature metadata has been considered less privacy invasive than the actual data being transmitted’ (Hoepman, 2021, p 100). As Mayer, Mutchler and Mitchell (2016) observe, in the US if a government agency wishes to release the content of personal communications it must ‘comply with extensive substantive and procedural safeguards’ whereas a law enforcement officer could request telephone calling records with just a subpoena, in other words, a formal letter (Mayer, Mutchler and Mitchell, 2016, p 5536). And yet, while individual telephone calling records may be of relatively little consequence, the bulk release of telecommunications data

can have ‘significant privacy impacts’ associated with surveillance. Contrary to claims that metadata is not personally identifiable information ‘telephone metadata is densely interconnected, can trivially be reidentified, enables automated location and relationship inferences, and can be used to determine highly sensitive traits’ (Mayer, Mutchler and Mitchell, 2016, p 5536).

The power of metadata to identify an individual and their behaviours was well illustrated by a panel at John Hopkins University in 2014 involving David Cole, security expert and lawyer, who when asked to speak about the privacy impacts of metadata, questioned the sincerity of President Obama when he repeated the ‘mantra’ that:

We’re [the US government] not listening to your phone calls, we’re not listening to the content. We’re just collecting the metadata, which means, who you called, when you called them how, how often you called them, how long you talked to them for. That’s all we’re collecting, just the metadata, so you shouldn’t need to worry about it.

Instead, Cole suggested he would rather ‘take his cue’ from the former General Counsel for the National Security Agency for the US who said on this question that ‘metadata absolutely tells you everything about somebody’s life. If you have enough metadata, you don’t really need content. It’s sort of embarrassing how predictable we are as human beings.’ To which Cole’s fellow panellist General Michael Hayden, a former director of the NSA and the CIA, went a step further, saying that not only was Baker’s comment ‘absolutely correct’ but that ‘We kill people based on metadata’ (YouTube, 2014a).

Compared to telephone call logs, WhatsApp collects far more information on its users’ behaviours. The World Economic Forum makes a distinction between different types of personal data based on their source. In its ‘taxonomy of personal data’ it identifies: *Volunteered* data as data you create and reveal deliberately and explicitly, such as social media profiles; *observed* data as data that is captured by recording the actions and behaviours of individuals and that you therefore reveal implicitly through your use of a service or device; and third, *inferred data* which is data about individuals based on analysis of volunteered or observed data as outlined earlier such as credit scores (World Economic Forum, 2011, p 9 cited in Hoepman, 2021). Hoepman clarifies that when we talk about metadata we therefore mean ‘observed data’.

As we argued in Chapter 5, the public response to WhatsApp’s privacy policy in 2021 increased awareness among some in the Indian public about what kind of data WhatsApp collects about its users’ relative to other private messaging apps, how data has been shared with Facebook since 2016 and what it was doing with that data. In response to user concern and media

reporting, WhatsApp went to greater lengths to be more transparent about the kind of information that users volunteer and it observes through ‘automatically collected information’. Here WhatsApp makes a distinction in its privacy policy between ‘user content’ that is encrypted and that which is not. For example, ‘messages, media within messages and calls’, Status information and Precise Location Information are encrypted. While profile pictures, names and descriptions of communities and groups and the use of avatars as well as the photos used to generate these are not encrypted.

When it comes to the observed data WhatsApp states that there are ‘certain types of information which are required as part of the Terms of Service and without which a person will not be able to access the service’. Some data is optionally shared in order to access additional features and services, such as the location information sharing. We know that the basic information that all users provide to WhatsApp or that WhatsApp collects, concern: a mobile phone number, information about a users’ activity, how users interact with others using WhatsApp and the time, frequency and duration of activities. WhatsApp can also see what features you use like messaging and calling, the status as well as avatars, communities, groups and business features. WhatsApp collects information about whether you are online and what time you were last online and when you send and receive calls and messages and when the ‘about’ information was last updated.

In addition to ‘usage information’ WhatsApp also records information about users’ devices, including what kind of phone they use and operating system as well as the battery level, signal strength, app version, browser information and mobile network. WhatsApp can also see the kind of internet connection being used, ‘whether that’s wifi or cellular data, mobile operator or internet service provider (ISP), language and time zone, IP address, device operations information and identifiers (including identifiers unique to Meta Company Products associated with the same device or account)’. Even where users do not use the location sharing features WhatsApp nonetheless collects the IP addresses and additional information such as area codes that enables them to estimate a user’s general location. WhatsApp also collects information about ‘user choices’ which relates to in-app settings, privacy settings and when you accepted the terms, whether users have enabled push notifications or employ disappearing messages (WhatsApp, 2024a). All this amounts to a considerable number of data points that can be aggregated and analysed for commercial insights and value.

Although WhatsApp is not *in* the digital living room, they are the hosts and let people in the front door: WhatsApp can work out who is in the room and when, how long people meet for, from where they join and how frequently they meet, among other things. Zuckerberg and Sandberg reportedly deliberated about the risk of ‘leaving money on the table’ when learning that end-to-end encryption was in development for WhatsApp,

however they would have been very aware of the value and power that WhatsApp's metadata alone would generate for Meta. Metadata is highly sensitive and when aggregated and analysed to produce 'social graphs' it can be used to predict people's relationships and behaviours which is valuable information for targeting ads and influencing decision making. Crucially, compared to the content of personal messages, voice notes and calls, whose meaning is not only bulky to store but also highly contextual and hard to interpret, metadata is more structured. The structured nature of metadata makes it easier to store, easier to analyse and easier link to other data than unstructured data content ([Hoepman, 2021](#), p 105).

For example, using a western cryptography allegory, if Alice speaks to Bob, then goes to visit him and stays at his place over night and a few days later is sending messages to a number which belongs to an abortion clinic and the day after Alice visits the location of the clinic in person then you do not need the content of the messages to figure out what's going on in Alice's (and Bob's) life. WhatsApp could infer this information because when at the same place Alice and Bob's devices would be connected on the same network, the location of both phones would remain the same over a period of time, data is collected about who speaks to who and when at the clinic Alice's location data or even connection to the clinic's WIFI would reveal her location.

When the lawyer Kapil Sibal appeared for WhatsApp in a 2017 hearing on the data protection framework of WhatsApp he evaded questions about what data was shared between WhatsApp and Facebook by reiterating 'that far more data is being shared on Google' to which the bench 'expressed its disapproval, noting that merely because other entities did it, did not make it a correct practice' ([SCO, 2017b](#)). The point is that despite the content of messages being end-to-end encrypted and therefore private, WhatsApp is not as private as it could be by default (also see [Burgess, 2023](#)). It does not need to collect so much data, volunteered or observed.

Take Signal for comparison. Co-founded by Brian Acton and Moxie Marlinspike in 2018, Signal is a not-for-profit private messaging service that runs a privacy focused messaging app but operates a more minimal approach to data collection. Responding publicly to a subpoena from the Eastern District of Virginia in the US that required Signal to provide information about two Signal users for a federal grand jury investigation, Signal issued the following statement:

We've designed the Signal service to minimize the data we retain about Signal users, so the only information we can produce in response to a request like this is the date and time a user registered with Signal and the last date of a user's connectivity to the Signal service. Notably, things we *don't* have stored include anything about a user's contacts (such as

the contacts themselves, a hash of the contacts, any other derivative contact information), anything about a user's groups (such as how many groups a user is in, which groups a user is in, the membership lists of a user's groups), or any records of who a user has been communicating with. (Signal, 2016)

What is significant is that because Signal has a minimal approach to data collection it could not respond in full to the request from the Eastern District of Virginia to supply information about Signal users, thereby protecting their privacy interests by default. By contrast the collection of users' data by WhatsApp presents the potential for not only WhatsApp to draw on this data, but for it to be accessed by law enforcement agencies. Moreover, 'WhatsApp actively cooperates with law enforcement authorities in India and continues to take steps to assist in their efforts to keep people safe'. To do this, it 'has a dedicated team of individuals who review, validate, and respond to law enforcement requests for user data in India' ('WhatsApp LLC V/s Union of India (Special Leave Petition)', 2021).

But if WhatsApp intends to operate with users' maximal privacy interests in mind, then why does it collect more metadata than it needs? WhatsApp outlines that 'You share your information as you use and communicate through our Services', and we share your information to 'help us operate, provide, improve, understand, customise and support our Services' (WhatsApp, 2024a).

But others have questioned whether WhatsApp even needs to collect all this data just to run the service and how that data might be used down the line by different actors. In our interview with tech journalist Aditi Agrawal, she proposed that WhatsApp's collection and aggregation of metadata is a business- or competition-related issue as much as it is a privacy matter.

Facebook has a lot of metadata that it collects directly through its different services (Facebook, Instagram, Messenger) and indirectly through all the plugins, ad measurement tools it offers to a host of service providers across the internet. And these signals are very important from a business standpoint. And once you start collating it with WhatsApp metadata, you get a lot of information and a lot of insights into how consumers are interacting with different brands. And there is a qualitative difference between how users interact on Facebook or Instagram and how they interact via WhatsApp. The latter is seen as a more private, intimate way of one-to-one communication compared to Facebook and Instagram which are about public messaging. And that does give Facebook, sorry, Meta a competitive advantage. For instance, tomorrow, if Meta wants to start, ... an online travel booking service such as MakeMyTrip or Kayak, Meta, through Facebook, Instagram and WhatsApp, already has a lot of data about how they interact with

their users. MMT, for instance, uses WhatsApp for Business to send travellers details about their bookings. This can either be used by Meta itself for its competing, hypothetical travel service, or be sold as insights to data brokers. You start collating those data points and you get insights. So it may not be data specific to say Philippa or Lipika or Aditi. But it will give you certain trends about this person interacts with the MMT service. Meta also gets details of how this person interacts with a particular business that sells women's shoes. This person also interacts with this particular business that sells ... I don't know, scented candles. I'm going with stereotypes here, forgive me for that. And this person also engages with this business that sells pet-related paraphernalia. I, as Meta, don't need to know who this person is. But I do know this person is potentially a female or female presenting and has pets and potentially travels a lot. I don't need to know who that person is, but it is a type. It's the problem that we have with non-personal data aggregation as well. You may not have data specific to Indians but you will have this kind of a cosmopolitan/globalised consumer profile that is of immense value to all kinds of advertisers, data brokers and law enforcement agencies.

The truth behind WhatsApp's approach to metadata concerns the fact that for WhatsApp, privacy is the distinctive 'feature' they use to sell their product, but privacy alone does not make the company money. However, as Aditi Agrawal went on to argue, WhatsApp's promise of privacy has 'certainly helped mitigate Facebook's bad reputation'. Defending users' privacy by suing the Indian government over not breaking end-to-end encryption, and taking a firm stance on this in places like the EU, US and the UK, as well as in Australia, New Zealand and Canada has 'been a really, really good PR exercise. I don't know if it's as altruistic as just caring about users. I don't think it's that easy. There are vested interests. It's not as pure as we're the upholders of privacy.' Moreover, 'if that were indeed the case, the privacy policy would not look the way it does now.' As Aditi says, WhatsApp wants to 'have their cake and eat it too'. In other words, they use their commitment to end-to-end encryption to promote WhatsApp as a 'paragon of privacy' while the privacy policy consent mechanism permits them to 'monetise the meta data without breaking end-to-end encryption'. This keeps Facebook happy because 'metadata is very, very valuable for law enforcement as well as from a commercial perspective'. 'The introduction of ads in the Updates tab is the latest blow to WhatsApp's promise of privacy,' Aditi said.

The privatization of India's digital private lives

As we documented in [Chapter 5](#), the amendments to WhatsApp's privacy policy and its progressive acquisition and sharing of metadata activated

questions of data sovereignty and data colonialism in India. The privacy myth that it is ‘merely metadata’ and therefore not of concern for individual privacy rights is perpetuated by wider mythologies of ‘big data’ and the asymmetrical power relations that exist between data producers and owners – end users and app developers (Thatcher, O’Sullivan and Mahmoudi, 2016). As we explained earlier, individual data is valueless and meaningless *until* it is amalgamated with other individual data points to analyse the temporal, spatial and networked characteristics. Given the enormity of aggregated or ‘big data’ sets algorithms do the work of selecting, interpreting and analysing what data to include and exclude. Decisions about what (individual) data is meaningful and what is and is not collected ‘do not occur in a vacuum’. Instead, data creation and exchange are ‘processes of capitalist accumulation by dispossession’ whereby ‘[p]reviously private times and places are commodified and privatized as a new terrain for capital investment and exchange’ (Thatcher, O’Sullivan and Mahmoudi, 2016, p 994).

Whereas Bumble or TrulyMadly privatize dating and romantic meetings and Swiggy privatizes and commodifies our food preferences and delivery addresses in India, WhatsApp privatizes and commodifies the data points generated by users sharing private encounters and information in and between its digital enclosures. So, what we share, when and with whom. WhatsApp has privatized our digital privacy itself. It is the architect and host to digital private enclosures and as the private authority has ultimate control over the rules of access to these spaces: it can influence behaviour within digital spaces (for example by adjusting the friction on the ease of sharing information) and determine the data it collects and shares, all of which they can alter at any time.

Following the public backlash to its privacy policy update and user concern about the limits to their experiences of privacy on WhatsApp despite the existence of end-to-end encryption, WhatsApp ‘built in’ a series of additional privacy features. We discuss privacy experiences in more detail in Chapter 7, but suffice to say here that WhatsApp’s new privacy affordances were intended to give users more ‘control’ over and reassurance about their privacy on WhatsApp through ‘interlocking layers’ of protection which included: disappearing messages, chat locks, the ability to silence unknown callers, encrypted backups and the choice to customize who can see when you’re online and when you last used WhatsApp. The affordances were designed to offer users more ‘granular control of their privacy and conversations so that secrets stay that way’ (Bapna, 2023). As stated on WhatsApp’s webpage, ‘Whether it’s your confessions, your difficult debates, or your silly inside jokes, your conversations need to be protected’ (WhatsApp, 2025g).

The addition of ‘built-in’ privacy features were part of a new global privacy campaign for WhatsApp that was given local expression and ‘monumental’

publicity through a 3D anamorphic installation filmed at the Gateway of India. The two-minute film opens with a time lapse of the Gateway of India in Mumbai and bustling audio as people mill around two giant cube structures that are under construction on either side of the gateway and on which 3D anamorphic immersive films will appear. The film then cuts to black and goes silent before the same scene at night reappears; now the precinct is empty, and the giant 3D anamorphic installations and the Gateway of India are lit up. An audio of WhatsApp's familiar notification alert signifies the arrival of a WhatsApp message, represented by a sealed green envelope. This initiates a sequence that depicts the envelope's journey while telling a story about how one can 'message privately with multiple layers of protection'. Iconic Mumbai sites and features locate WhatsApp in India and in the city.

The message first travels within the privacy of a '*kaali peeli*' (black and yellow) taxicab which is transformed by a splash of WhatsApp green paint upon the envelope's arrival. The taxicab represents the end-to-end encrypted nature of personal messages that 'no one can see or hear' – remember the container metaphor described previously. As the message floats off out of the car window past the Gateway of India it lands in the aperture of a red post box, a legacy of British colonial power, and used here metaphorically to signal two step verification to access WhatsApp chats so users can stay 'two steps ahead of intruders'. The envelope then floats past Mumbai's high-rise skyline as the sound of sirens and crowds fills the audio and we learn about the capacity to 'silence' unknown callers and 'screen out spam'. A pigeon clutches the envelope in its feet for the last leg of its journey before disappearing mid-air in a cloud of feathers, demonstrating the presence of '[d]isappearing messages, chats that self destruct'.

Finally, the message itself is revealed: 'Hey, meet you at the Gateway of India in Mumbai' and the recipient replies 'Great! See you at 7pm'. The camera pans round to centre the Gateway of India which is lit up in WhatsApp green with a white pad lock projected on to this iconic monument accompanied by the sound of a padlock closing (see [WhatsApp, 2023](#)).

Sandhya Devanathan, Head and VP, Meta in India contextualized the motive for [WhatsApp's 2023](#) privacy campaign:

Privacy is at the core of everything we do at WhatsApp. We're excited to see the next phase of our privacy campaign light up the Gateway of India and raise user awareness around WhatsApp's privacy features and multiple layers of protection. The eye-catching, one of a kind anamorphic privacy installation uses innovative and immersive storytelling in true Mumbai style to reinforce WhatsApp's continued commitment to launch features that strengthen our existing layers of protection, giving people full control over the level of privacy they need while messaging their friends and loved ones. ([Meta, 2023a](#))

In an interview for the marketing publication *Drum*, Devanathan summed up the logic behind the campaign: '[t]he genesis behind our privacy showcase at the Gateway of India was to create an unforgettable immersive experience to bring WhatsApp's privacy features alive' (Bapna, 2023).

The advertisement spatially embeds WhatsApp's private digital spaces within Mumbai's cityscape, signified through the hyper-local icons and landmarks as the private communication – the envelope – floats through the city. The personal information remains concealed while in transit, but its temporal and spatial data points are known, to us the viewer and therefore also WhatsApp. Only on arrival is the communication shared and after which a giant stylized padlock is lit up on the Gateway of India. Built to celebrate the arrival King George V for his coronation in 1911 as the Emperor of India, it was also the archway through which British troops left India in 1948 following Indian Independence in 1947. WhatsApp's projection on to the Gateway of India simultaneously signals the 'privacy layers' available to users to 'control' their personal information, which must be 'protected'. At the same time, WhatsApp's green chromatic capture of each of the landmarks along the route, culminating in the illumination of one of India's iconic landmarks of independence bears a certain irony. It could be interpreted as a metaphor for Meta's neocolonial power over the vast quantities of data generated from the everyday digital private lives of India's citizens.

There are two key issues at stake here. The first concerns how WhatsApp orientates its campaign around privacy design features and privacy-as-control. In response to public concern about data privacy on WhatsApp, the company chooses to reiterate to users that their communications 'need to be protected' and that WhatsApp's new privacy design features will enable individuals to have more control over their private digital environments. On the face of it, greater control for individuals must surely always be a good thing, no? But as privacy lawyer Neil Richards contends, privacy-as-control is in fact 'an illusion' and a 'highly appealing one'. 'When a company's response to a privacy scandal is "more control", this simply means more bewildering choices rather than fewer, which worsens the problem rather than making it better' (Richards, 2022, p 93). New privacy features make for a compelling campaign story and create the impression that WhatsApp truly cares about users' privacy but it also 'distracts us from the real problems of power and manipulation' (Richards, 2022, p 93). Ari Waldman reminds us how Big Tech's privacy designs and architecture in combination with discourse play a role in misdirecting our attention. So while we are distracted by the publicity around WhatsApp's new 'privacy layers' and 'privacy controls', the company is busy 'undermining our privacy' in other areas (Waldman, 2021, p 57). In this case, keeping out of view the metadata it collects, the 'vast iceberg of dark data existing below the waterline of our comprehension' (Richards, 2022, p 97).

Second and relatedly are the asymmetrical (and contradictory) power relations that come ‘alive’ in [WhatsApp’s 2023](#) privacy campaign. The chromatic capture of the Gateway of India could be read as the fruition of Zuckerberg’s project to connect the ‘rest of the world’ and conquer its access to the Indian market. On the one hand, WhatsApp’s privacy architecture legitimizes its claims to design and strengthen a digital privacy infrastructure that socially and economically empowers India while on the other hand, that same infrastructure simultaneously extracts Indians’ metadata and transforms it into a powerful private resource that fuels WhatsApp and Meta’s economic and political growth. The sheer bigness of WhatsApp’s network and data further entrenches WhatsApp’s (and therefore Meta’s) private authority in India and beyond.

Conclusion

Escobar argues that most design, whether of consumer goods or digital technologies, architecture or policy, ultimately serves capitalist ends. In the context of WhatsApp and India, this chapter was interested in how privacy ‘design’ is a ‘situated and interactive practice’ ([Escobar, 2017](#), p 40). By focusing on WhatsApp’s implementation of end-to-end encryption as a proxy for privacy, we have shown how privacy-by-design carries a form of code power in its negotiation of personal and geopolitical relations. But as a novel, invisible technical code among ordinary users, end-to-end encryption needs domesticating through metaphor and media campaigns to cultivate trust in digital privacy as the product and keep users ‘picking up’ and sharing on the app. Yet, as we document, these curated metaphors and stories universalize and normalize privacy experiences sometimes in ways that contrast with or contradict participants’ situated experiences of privacy and WhatsApp in India and can serve to reproduce inequalities (see also [Chapters 4 and 7](#)).

WhatsApp importantly uses end-to-end encryption as a ‘privacy thing’ that draws attention towards the significance of users’ personal messages while deflecting attention away from the value of metadata that WhatsApp collects every time someone engages with the app. In this era of Big Tech and big data, Paola Ricaurte proposes that we ‘reframe ... colonial power in terms of data colonialism as an epistemic order based on data’ which, as a form of extractivism ‘assumes that everything is a data source’ ([Ricaurte, 2019](#), p 353). Embedded within India’s social, political and economic fabric WhatsApp actively collects terabytes of data on the behaviour and practices of its users across everyday life which can be processed and analysed to derive new value. In conjunction with the arguments presented in [Chapter 5](#), we argue that the paternal overtones that characterize WhatsApp’s articulation of code power and its promotion of privacy infrastructures are also ‘an expression of the coloniality of power’ ([Ricaurte, 2019](#), p 357). WhatsApp’s promise to

prioritize India's economic needs and protect its (privacy) interests serves its own private interests and authority. Yet, despite WhatsApp's asymmetrical power relations Indian citizens and activists critically engage with the limits of the app to serve their situated privacy concerns, mobilizing both anticipated and anticipated features to do so, as we explore in the [next chapter](#).

Privacy Is (Geo)political

The book's opening provocation questioned *whose* digital private future was Mark Zuckerberg imagining when he announced (then) Facebook's pivot towards a digital private future. [Chapter 5](#) expanded on the material, ideological and (geo)political manifestations of his privacy vision as mobilized through WhatsApp. In this chapter we begin from a different vantage point to understand how citizen-users have interacted with WhatsApp's privacy architectures in the formulation of their everyday ideas, experiences and practices of (digital) privacy in India. Concerned with how digital technologies 'land' in the 'digital peripheries' we question not only how WhatsApp has shaped India's digital privacy landscape but how India has shaped WhatsApp's privacy architecture too. To do this, we integrate approaches concerning the social life and meaning of privacy, how digital technologies become 'domesticated' and how privacy is worked and re-worked in everyday life. Social theories of privacy support a decolonial and feminist geopolitical approach that values interpreting privacy from the 'bottom up' to 'avoid the generality problem of *a priori* theories and allow privacy to evolve with changing values, culture and technology'. And, importantly such an approach conceives of privacy as a social relationship that is struggled over, negotiated and 'embedded in daily social life' ([Waldman, 2018](#), pp 36, 43, see also [Solove, 2002](#); [Nissenbaum, 2009](#); [Marwick, 2023](#)).

As such, this chapter documents how digital privacy is not just intrinsically political but also intimately geopolitical in its affect and experience, particularly as privacy is shaped within existing structures of power and social hierarchies. The work of [Elwood and Leszczynski \(2011\)](#) on the impact of geospatial technologies on privacy is particularly valuable here for recognizing how WhatsApp is implicated in the stories and struggles over digital privacy which involve the ongoing (re)configuration of roles and relationships between citizens, civil society, the state and digital technology companies.

Second, the chapter integrates social theories of privacy with a sharper focus on the materiality of privacy. [Nippert-Eng's \(2010\)](#) sociological study

of privacy in the US implicitly documents how ‘privacy things’ – wallets and purses, cell phones and email, windows and doorbells – are inherent to people’s privacy meaning-making practices. Drawing on ‘domestication’ theories and its critiques supports our examination of how WhatsApp’s privacy architectures have been ‘tamed’ or appropriated within the culturally specific context of the ‘digital living room’, the home and everyday geopolitical life more broadly (McDonald, 2015; Silverstone, 2006). We are concerned with how citizen-users interpret, negotiate and experience WhatsApp’s privacy promise and ‘privacy things’ within the wider context of their digital and sociopolitical lives. Attentive to how the domestication of WhatsApp in India is by no means a unilateral process, the privacy stories documented here raise important questions about how digital technologies are repurposed and engaged with in unanticipated ways in the ‘digital peripheries’ (Chan, 2014; Poggiali, 2016). This approach critiques not only western practices of privacy and surveillance but also post-colonial state practices of surveillance (Arora, 2019c).

Finally, by foregrounding the privacy stories of WhatsApp’s citizen-users we gravitate towards the role of people’s agency in designing and redesigning privacy in context. This productively engages with Alice Marwick’s concept of ‘privacy work’, Nippert-Eng’s idea of ‘boundary work’ and ‘learning’ privacy norms and practices and Arora’s appeal to centre more ‘playful’ privacy practices which variously speak to the ongoing labour invested in realizing privacy and private lives (Nippert-Eng, 2010; Arora, 2019a; Marwick, 2023). The privacy stories call into view the intimate tension between privacy, safety and surveillance that minoritized individuals in particular must navigate under patriarchal, generational and heteronormative structures of power. Through this, we examine the emotional and material harms that are at stake when privacy is at risk, the emotional political economy of digital privacy and the intersecting roles and responsibility of different state, corporate and society actors. Understanding ‘privacy work’ in this context nuances readings of the global north and south as the ‘privacy rich’ and ‘privacy poor’ to unpack the situated work associated with achieving a sense of digital privacy within intimate geopolitical spaces.

We begin by contextualizing the meaning of privacy in India through people’s privacy stories before turning more explicitly to the case of WhatsApp to examine how end-to-end encryption as a ‘privacy thing’ has been domesticated. The third section develops our argument that digital privacy is geopolitical by locating experiences of WhatsApp and digital privacy within the context of family and community, state and corporate surveillance. The fourth section documents modes of privacy work on and around WhatsApp and the chapter concludes by considering the implications of privacy work as privacy by redesign.

Privacy stories: what does privacy mean?

From the outset it is worth stating that participants took privacy seriously; privacy was not a foreign or irrelevant idea though how privacy and the private were interpreted and situated within people's lives varied. A popular response conceptualized privacy in terms of solitude or having the option to be alone which was also coupled with the ability to control information flows about oneself. Ipsita, who was in her mid-twenties with aspirations to study for a master's abroad, initially hesitated before surmising that '[p]rivity is basically the idea of being left on your own and not having to explain or tell anyone what you are doing or what you are thinking about or what's going on'. Moreover, privacy concerned autonomy and control over the information available about oneself as she went on to explain that privacy is 'being able to divulge as much information as you want and when you want or choose not to reveal any information about any aspect of your life'. Shivi, a woman in her mid-forties who came from a Hindu family and owned a small beauty parlour, agreed: 'First thing, it is very important. In every possible way. Like, I mean I need my privacy for my own mental health, wellbeing and also just to be myself. So, privacy is also important because I get time for myself with myself, you know.'

For other participants, privacy was also spatial, some referred to privacy as a 'zone' which was beyond the surveillance and intrusion of 'third parties' or 'unwanted' others and as such granted individuals a feeling of comfort and security. Harpreet came from a Sikh family, worked for a gaming company managing peoples' data and was at that stage living with his parents in their house in East Delhi. He explained that as a single child he had a separate room and his parents would always knock before entering, recognizing that he might be working and not want to be disturbed. This was important for Harpreet who regarded himself as a private person and explained that he valued his private space as somewhere he could be in his 'comfort zone you know, where I can do anything without really thinking about what somebody else is thinking about you if anybody else is there ... it's where I can do anything without thinking about anything'.

Arman, a law student, also emphasized the importance of his private space within the home that he shared with his parents and siblings in the Muslim majority neighbourhood of Jamia Nagar in South Delhi. Arman explained that 'private space' is 'where you can do anything without someone actually having the capability to keep a track of you or use that [information] to do whatever it is against you later on'. He keeps his room closed most of the time which his family initially questioned, 'but now they don't mind' and he feels safe knowing that they are busy in their lives and won't intrude on this space. Arman explained that for him, privacy was important because 'It gives me the freedom to do whatever I want to do without the fear of

being judged, or without the fear of being analysed. ... It allows me a space to develop my individuality, to do things which I wouldn't dare to do in front of anyone else.' A private space was therefore somewhere to develop a sense of one's identity and to experiment without fear of judgement. As Raima who was also from a lower-middle-class family background agreed, privacy 'is something that gives people confidence and freedom'.

Yet, accessing personal or private space was not possible for many. Bahir Ali recalled his experiences growing up with his parents and five siblings in a Muslim majority neighbourhood in southwest Delhi where they shared a small two-room house. He described the challenges of 'creating a space' for himself where:

One of them [the rooms] was a common sitting area where some of us would sleep and upstairs in the other room me and my brothers would sleep. There wasn't any privacy at that time. I used to find a corner spot for some private space. But it wasn't very private as anyone could enter the room and we couldn't even lock it. We used to sleep together and not alone so that cuts at the very root of privacy for self. Creating a space for myself has been a struggle until I got married. Not just me, my siblings and even my parents could not achieve private space back then. Now since we have moved to another house, a bit of privacy can be maintained but six months back, privacy was not in existence [giggles].

Private space was conceptualized in terms of material and figurative boundaries which were variously determined depending on the nature of relations or information. For instance, as Malavika, who worked as an advocate for digital justice with an NGO explained:

For me, privacy is, quite simply, a form of boundary, one that I don't want anyone to cross. Within this boundary lies my data, my information, my decisions, my body, my thoughts, and even my voice. It's all part of what I consider personal and off-limits. Sometimes, it even feels like my phone is monitoring and listening to me, and that, to me, is a violation of privacy.

Such boundaries were continually navigated and degrees of privacy maintained among different social relations. Jamaal lived in a house with his same sex partner and explained how he 'negotiates these kinds of private activities'. When at home, his phone represented a site of privacy from his partner, though they shared everything else within the home. However, they kept their relationship private from their parents anticipating their disapproval, and the fact that they lived together was private not only from

their parents but many others too, to limit the potential risk that information about their circumstance might leak.

For Bahir, it was important that his close relations were aware of the implicit boundaries that ‘nobody can cross’ and that defined his privacy for example:

Whether it be my wife, she cannot peep into my WhatsApp and check who I am chatting with. Or my parents, they cannot look into where I should go or not. That is solely my choice ... I mean everybody has their own life ... A set of boundaries should be created in everybody’s life ... No one should cross it, but when someone does, I get angry, upset and hurt. That set of boundaries is privacy for me.

Importantly, the act of crossing boundaries was understood to provoke strong feelings for those wishing to preserve their privacy. Sanya, a social media content creator in her late teens recalled a formative experience when her privacy was violated. As a child she was an avid diary writer, recording her intimate feelings ‘from all the corners of my life. It was so private for me that I didn’t even read it afterwards.’ Then one day her family decided to sell some of the books in her room and when she returned, she found her father reading her diary. As she explained: ‘I felt weird not because my secrets are now known to my father but because it was such a private thing for me. He looked at me while saying a few words mocking at my stupid incidences. He put the diary down and left.’ After that incident Sanya made one last entry in her diary. She recalled how she wrote:

Today, my father has read my diary and drew a broken heart. As soon as I wrote this, I tore it and as it was winter I put it in the bonfire burning outside. After that I did not write any diary ever because this breach of privacy was very weird for me to accept. Everyone knew that I used to maintain a diary and I did not want anyone to read it, in fact, I had even fought with my younger siblings to prevent them from touching my diary. I had told my mother specifically that no one should read my diary. Still that incident happened and my privacy was strongly violated.

Though Sanya had since attempted to revive her daily writing on her phone ‘that one incident left a long-lasting impact’ which left her feeling fearful of future privacy violations.

Like Bahir and Sanya, the salience and socialization of privacy was something Hiba developed through her childhood. Hiba, a middle-class woman and the daughter of Hindu-Muslim parents, spoke about how the concept of boundaries, surveillance and private space was implicitly shaped by observing her mother’s ‘ritual’ behaviour whereby ‘in the morning she

would open the curtains, in the evening she will close the curtains, so that's one of the first things I picked up, without really understanding, or picking up the word privacy ... I picked up about what is sacrosanct, what is public and what is private'. In addition to shaping the materiality of private space, Hiba recalled how their mother would also speak in hushed tones, even when inside, when discussing particularly sensitive topics and 'she would shush us and be like, "no, no talk softly, neighbours will hear, neighbours will hear"'.

The importance of 'non-interference' or minding one's own business was evoked by other participants too. Ranjit was a security guard in his mid-forties who had recently moved from the northern hill town of Nainital to work in New Delhi. While 'privacy' and its literal though rather technical translations *gopniyata* or *nijta* did not immediately land with him, he did recognize the concept of privacy in terms of 'niji mamla' (a private matter) and 'personal baat' (a personal thing). What resonated more directly was the importance of personal space that was free from interference and disturbances. But Ranjit was keen to emphasize that this required free time which he, as a labourer, did not have a lot of, and space, which was also under pressure in the city. He replied somewhat rhetorically 'Empty place with silence and without any disturbance, where will one find it?' before qualifying that 'somebody will come and be a disturbance. All the places are full of public.'

The views of New Delhi participants echoed some of the opinions expressed on Nitin Sethi's X (formerly Twitter) thread that we introduced in [Chapter 2](#). These views concerned the apparent novelty of 'privacy' within India, which was attributed to Indian society being embedded in community and familial ties whereas western societies are more individualistic. Ipsita explained that 'in theory, yes', the right to privacy is there 'but in practice, it's not. A lot of it concerns how our society is constructed ... there is no concept of privacy in our culture from the beginning because we are a more social like community-based society and community-based culture.'

Similarly, Sanya, who worked in a beauty salon in New Delhi believed privacy was a right.

It is there, but in limited spheres. There can be privacy in each and every sphere of our life, from my phone to bag, to even a cup; if I don't want someone to touch my cup, it is my privacy. But very few people understand this ... Although people are educated, they don't know privacy. They would check someone's phone without permission. In our salon, boys and even girls would take out stuff from each other's bag without permission. I have told them about privacy but they made fun of me saying it is fine with friends and that there's no privacy among friends to which I say it is absolutely not necessary for friends to know each and every thing and hence privacy can be maintained. But they don't know, they haven't ever learned about this; actually no

one has ever told them about privacy. In schools, we are not taught about privacy. ... And when they don't know about privacy, they end up disrespecting the privacy of others.

Sanya went on to explain that privacy was something people had to learn, whether in school or from each other. She gave the example of a potential marriage match she was getting to know and who she felt had unreasonable expectations that she should share everything with him, like her passwords. But as she explained:

Why should I give? We are not married! And even after marriage why should I share my password with you, that's my private thing. I don't want to share. There are a lot of things related to privacy There's nothing wrong or secretive in it as such, just little things in life, but I don't want to share it.

Others challenged the perception that privacy was not an indigenous concept within India. In an interview for the project, Arvind Narrain, an academic and legal scholar, argued that 'people find their sense of privacy in the Indian context' and drew on the example of the Kannada and Dalit poet, Siddalingaiah whose poetry was inspired by his experience as a young boy seeking 'a sense of peace, a sense of quiet' within graveyards. Recognizing how this place or 'zone' brought privacy and sanctuary for Siddalinghaiah, Arvind also reflected on the risk that sexual and gendered minorities can also be 'hemmed in' by private spaces which can also curb one's right to autonomy.

In addition, acts of 'boundary making' and controlling information flows to protect one's identity, freedom and autonomy are not new for many of India's citizens who have long been the subject of surveillance by their family, the community and the state (Phadke, Khan and Ranade, 2011; Arora, 2019c). Readers familiar with the Indian context will not be surprised to learn about the experience recounted by Raima, who regarded privacy as critical for her safety and wellbeing within the patriarchal and heteronormative political culture of Hindu nationalist India. Despite her Hindu sounding first name, Raima was a single Muslim woman from Meerut, then living in New Delhi. Earlier in her career Raima recalled how she regularly travelled out of the capital for her job as a health worker which took her to the more rural states of Madhya Pradesh and Uttar Pradesh and when doing so:

I used to not tell my complete name to people, especially in the hotels where I was staying. Those small districts of Chitrakut and Banda, had shady hotels. So I would stay in the lodge or very small hotels. So it was a constant challenge for me and that was the first time I started

learning about how I can hide my identity and why I should hide my identity ... They [hotels] would ask me for my ID and I would just say that I have lost it. In smaller hotels, they were not worried about IDs so much ... I managed like that for two to two and a half years.

Raima considered how '[n]o one told me that I should hide my identity but I think I started feeling that if I tell my full name [Muslim surname], maybe the chances of violence with me are more'.

She reasoned that by concealing her full identity she was 'able to protect myself from violence faced by Muslims'. Despite her frequent travel Raima emphasized that 'I would never tell any of this to my family members. I have never told about this fear to anybody at home.' Raima also explained how she was careful about sharing information about her family. For instance, she always gave her office address, never a family home address and never shared family members' phone numbers. Strategically withholding information was twofold:

It is not just about somebody contacting them but also them getting to know about how I live my life. I don't want them getting to know it. ... So privacy for me is not just about protecting myself from people in the outskirts but also protecting from my own family, my community, my neighbourhood.

Raima's account illustrates her intersecting spheres of privacy which embodied slightly different risks. Raima was introspective about the importance of privacy and how her multiple identities contributed to intersectional vulnerabilities in Indian society: 'when it comes to privacy, for me the fact is that I am a woman, I am Muslim and I'm single'.

Drawing on research with marginalized youth in the US, Alice Marwick characterizes the ongoing labour that people like Raima engage in to protect their safety, identity and freedom as 'privacy work'. She determines that privacy is a 'social' and 'active process' that 'one engages in', 'to retain agency over what, how, and with whom they share information' (Marwick, 2023, pp 65, 66, 87). Marwick understands privacy work in partnership with what Liz Kelly, a sociologist specializing in sexualized violence, calls 'safety work', that is, 'the planning and strategizing that girls and women undertake to avoid men's violence'. Women engage in wide-ranging, often pre-emptive, behaviours to maintain their safety in public; in Kelly's words, safety work includes 'thinking processes, decision-making, and embodied watchfulness' (Kelly, 1987, cited in Marwick, 2023, p 66). As Raima's account testifies, her 'safety work and privacy work are closely related' (Marwick, 2023). Locating her approach within a feminist privacy protection framework, Marwick's research importantly

emphasizes that ‘some people are fundamentally denied privacy, that the harms of privacy violations are both contextual and differential, and that there are fundamental links between privacy and social inequality’ (Marwick, 2023, p 98).

Participants’ privacy stories illustrated marked shifts in their thinking about privacy. The Supreme Court judgment on the ‘Right to Privacy’ in 2017, the Cambridge Analytica revelations and the prevalence of media stories reporting on cybercrime, hacking and spam messages within the context of new digital technologies had raised the public profile of digital privacy, and privacy more generally. Ibadat, a female student from a middle-class Muslim family, remarked that because people were talking a lot more about privacy it had impacted her behaviour:

Earlier I was not concerned about it [privacy] at all. I thought why does it matter ... but now because everyone has been having a lot of conversations on privacy, so obviously I’ve started to think about it and realise what are the different facets of it, if it is not guaranteed or protected then what are the consequences if it is invaded? So I’ve gone from somebody not concerned about it at all to being concerned. So just an example, earlier there was a Truecaller issue. People used to say that they will take your data. But I had Truecaller and I was like it doesn’t matter. But now I have deleted it ... because of all the things that are happening.

Ibadat’s reference to Truecaller – a Scandinavian caller and spam detection app – illustrates how high-profile media stories operate to shift perceptions around digital privacy. Ironically, given that Truecaller is sold as an app that protects users’ security, media stories reported how ‘the majority of Truecaller’s datasets are comprised of information that has been collected without a user’s consent – a feat made possible by the lack of a comprehensive legal framework surrounding data protection in India’ (Khaira, 2022). For instance, if a person downloads Truecaller, it gets access to all the phone numbers stored in that handset without the user fully appreciating the scale of data breach or potential implications for those in their network. Similarly, Runa, a teacher in her forties, shared her uncertainty about navigating her digital privacy:

There are so many online scams and hackers and fortunately or unfortunately probably I don’t know, there may be advantages. But so much is online and beyond us right now. There is something which is really not under our control. And somehow there is that nagging fear that somehow something falls into the wrong hands, wrong project, or wrong image or financial transaction takes place.

This sentiment resonates with responses to a survey by LocalCircles, a digital platform that connects citizens with their local communities. It reported that 87 per cent of participants believed their personal details were in the public domain or leaked, with 91 per cent of people believing their phone number was in the public domain (LocalCircles, 2025). Corroborating those findings, a recent survey by the global consultancy firm, PwC on ‘India’s data privacy landscape’ reported that 58 per cent of people surveyed gave information but also kept ‘worrying about sharing it or wondering how they use it and what they do after using it’. This contrasts with 42 per cent of people who felt ‘obliged to give this information but have never thought about it’ (PwC, 2024).

People’s privacy stories illustrated how people took privacy seriously; it was struggled over as a social, material and spatial practice and was inflected by existing societal and state power relations. Noting the importance of context, privacy means different things to different people at different moments in their lives and can be a site of safety and sanctuary, as well as of struggle and harm. And as a practice that is learned and socialized within these different contexts, the stories about privacy implied how recent shifts concerning digital privacy had heightened people’s awareness of digital privacy but also privacy practices more generally. These stories (re)constituted privacy relationships between citizens, the state and Big Tech as we examine later in the chapter. How WhatsApp’s end-to-end encrypted messaging was received and domesticated within this context is the subject of the privacy stories we turn to next.

Domesticating digital privacy

Having established that privacy is a salient though diversely interpreted concept in people’s everyday lives we look at how WhatsApp’s promise of a *private* digital future is domesticated within everyday life in north India. As we described in Chapter 6, WhatsApp’s introduction of end-to-end encryption by default in 2016 transformed a novel security architecture into a mainstream technology. WhatsApp’s media and advertising campaigns actively exploited end-to-end encryption’s privacy capital by translating an otherwise technical and invisible code into a perceivable ‘privacy thing’. But how did people interpret the meaning and significance of end-to-end encryption when it came to their digital privacy?

People’s narratives about WhatsApp typically considered the *relative* privacy of the digital platform compared to other modes and spaces of communication. For Sanya, a dancer and social media content creator, WhatsApp was considered private compared to Instagram or Facebook because she knew who she was sharing information with on her closed groups: ‘To some extent, I feel it is a private space because the people on

my WhatsApp are well known to me and I can safely share photos and other data comfortably.'

Others were sceptical about the security of any digital interactions and more cautious in general about their privacy. Arman was circumspect about the potential for any digital app to offer privacy that could rival the privacy of his home.

No, in today's day and age nothing is a private space except for your home and whatever you do if there is no electronic gadget inside. That is what constitutes private space. When you are within the four walls of your house, nobody is there and there is no access to any electronic gadget, that's what constitutes private space. Apart from this, nothing really is private. WhatsApp is not private, in fact I wouldn't categorise any app as private; I wouldn't expect anyone else to respect my privacy to the extent that I do.

Like Ipsita, he perceived privacy as his responsibility and implicitly did not trust WhatsApp to be a truly private place, preferring to have sensitive conversations in person and taking care not to share information on WhatsApp that he deemed private: 'I usually don't really have the kind of conversation with anyone on WhatsApp which I feel should have been more private or something ... I prefer a face-to-face conversation and that's the only thing. I don't really have anything private on WhatsApp. It's just that I am cautious.'

Though Ipsita did not regard WhatsApp as private 'in the wider scheme of things', the app afforded her relative privacy within the family home as a place of escape where she could simultaneously be physically present with her parents while also seeking solace through her friends on WhatsApp.

But if I want to seek privacy from my family, then it is, yeah. Then I see then I can message my friends a lot. So, if I'm feeling low, if I've gone through a breakup and I don't want to talk about it with my family, then I will message my friends. I can be sitting in the same room with my parents doing my social obligation, but I can still message my friends on the side as to what I'm feeling.

She then went on to share how she was not entirely confident about 'the nature of privacy' and always had a nagging fear that her parents would access her WhatsApp messages on her phone. Aware participants typically knew that WhatsApp's messages were 'encrypted' but interest in or understanding about what encryption meant varied considerably. For many, 'encryption' was something that they were aware of but did not appreciate its consequence for them and their messages. As Savi reported, while she might have seen 'that notification come up many times but have never bothered to check what

it is' and Ibadat remarked that 'Yeah not that I know what [encryption] is. I just know that it is there.'

For a minority, WhatsApp's end-to-end encryption fundamentally informed their choice to use the platform. Preetam had a background in computer science and now worked for a gaming company. Portraying himself as a 'very secure person' he took his digital privacy seriously, for example by only engaging with websites that follow proper security protocols. He was impressed by WhatsApp's image and position as the leading social media platform to chat over the internet and moreover, the fact that messages were end-to-end encrypted. Preetam explained that:

End-to-end encryption is basically the current epitome of secure conversations when you are conversing with someone and basically, it's a public-private key player for chatting with anyone around the world. So in that case WhatsApp doesn't have access to any of my messages because the encryption of the message is done at the device level. And that encrypted message is sent over to WhatsApp servers and then WhatsApp sends that information to the receiver and that encrypted message and that device must decrypt the message. So in that case only the sender and receiver have the access to the information I am sending, not even the WhatsApp can store the information.

Preetam pointed out that there was an exception to this if the message could not be immediately delivered, then WhatsApp temporarily stored the encrypted message on its servers. He had not always been so impressed by WhatsApp; initially its association with Facebook undermined his and other's confidence in the app to protect people's privacy particularly given the negative media attention Facebook received in India. But its implementation of end-to-end encryption had altered that opinion.

Earlier I used to think WhatsApp wasn't a private space but that was because earlier it was a part of Facebook at that time and Facebook had been in the news a lot at that time because of scams. So I thought the same company is managing WhatsApp, so this is something which is not secure. But then they came up with end-to-end encryption which I know is the most secure way of communicating with someone. At present, I feel WhatsApp is a safe space for talking with anyone.

Preetam's thorough understanding of encryption technology and faith in WhatsApp's digital code to protect his privacy was unusual. It was far more common for people who showed some familiarity with encryption and understanding of digital privacy more generally, to still have a limited grasp of how WhatsApp's encryption architecture worked. People were cynical too

about the scale of publicity that WhatsApp gave to end-to-end encryption and were uncertain about the reliability of WhatsApp's claims that messages could not be accessed by WhatsApp nor the state.

Paras was a lawyer for a large international company who had used WhatsApp since its early days in India. He regarded privacy as both 'necessary' and 'a myth'. He puzzled over 'how much of it [privacy] we have nowadays, especially now with technology in our lives and with Facebook and WhatsApp and all the apps, financial apps'. He went on to question 'I don't really know how we can really keep things private anymore because at the end of the day one stores a lot of information online.' Paras had seen WhatsApp's ads for end-to-end encryption on YouTube but regarded it as 'a joke'. He went on to clarify his opinion:

I don't know, I think it is something that they [WhatsApp] advertise I don't really know if it is encrypted information that they still have access to. Maybe a third party doesn't, maybe they have made it a bit more difficult, but it doesn't mean that data doesn't exist. I think it can be deciphered and used, totally depends on your importance as a person and how important that relationship would be.

Like Paras, Raima, Jamaal and Ipsita understood the general purpose of end-to-end encryption but still believed that encryption could and would be broken in certain circumstances. As Raima remarked:

[m]y understanding is that when they [WhatsApp] declare [that messages are] end-to-end encrypted, they are saying that only the sender and receiver can see the message. But I think that is a bluff. That is not true. Maybe everyone can't access, but particular people can access, at particular times. So I don't think that is completely true.

Jamaal was a young gay Muslim man soon to study for a PhD in the US and who felt his physical, financial and intellectual privilege protected him from feeling like a minority. Following the backlash to WhatsApp's privacy policy update he commented on how 'WhatsApp has become this bad boy' and on end-to-end encryption he said:

I don't trust it. I don't trust anything for that matter, so definitely not end-to-end encryption. I feel like anything that's displayed in public, it's quite a sham so if they like very explicitly mention that something is encrypted, I don't know. I am pretty sure there is a backend team at WhatsApp who are ... not accessing ... but who are working with these chats. So even though there are machines ... there are people behind it. So it's never private.

Ipsita also humanized WhatsApp's seemingly abstract and technical infrastructure by considering the role of WhatsApp's employees when she shared her understanding of the app's security architecture:

What I understand is that only the people who are in that chat can retrieve it or have access to it. ... if a third person comes and asks WhatsApp, WhatsApp will not be able to give that information to a third party ... whether or not they pay. If there is a lawsuit that needs evidence then in that case, I also don't think it can be given. So, basically this is to say a WhatsApp employee who has certain access can't just randomly search what [we] are talking about ... but obviously there must be some way to get around it. Like it must be protected with certain checks which I don't know about. That is my guess.

She went on to comment that 'obviously end-to-end encryption is better and it does feel reassuring when an app has that message' but in other ways the question of whether end-to-end encryption was valuable for protecting her digital privacy was a moot point. Ipsita made it clear that she chooses not to share information on WhatsApp that she perceives as 'private'. For her, 'it doesn't matter if somebody sitting in a WhatsApp office knows if I have a boyfriend or I have this much money in my bank account ... generally I don't care a lot whether somebody or a random person knows this about me or not'. But for sensitive content, like 'nudes' that she doesn't 'want to go around even to random strangers' she uses 'hacks', for example by ensuring her face is 'never revealed' and 'there is no way to connect this to me' and she also 'takes [the photos] in a very neutral background space where there is no indicator of where I am or who I am.'

Despite WhatsApp's promise that 'End-to-end encryption means that no one outside of the chat, not even WhatsApp, can read, listen to, or share them [your messages]' (WhatsApp, 2025a), there was a persistent suspicion that encryption was a 'joke' and that at the 'backend' it was possible to decipher messages. Moreover, there was an assumption that 'particular people' or 'WhatsApp employees' could access messages in certain cases depending on who the user was and what their network was, in other words whether WhatsApp or the state wished to target them. When considering the extent to which WhatsApp was a private digital app, participants consistently gravitated towards the matter of whether their conversations *on* WhatsApp were private which engaged with WhatsApp's marketing around its product. Conversely, very few people questioned whether, or what, personal data was captured by WhatsApp and shared with Facebook and other third parties.

Privacy activists and journalists were also cynical about end-to-end encryption and mistrustful of WhatsApp's security intentions. Karmanya Singh, who had petitioned the Indian government over WhatsApp's

privacy policy updates, believed there was ‘a lot of faff around end-to-end encryption’ and made a distinction between end-to-end encryption which is security focused, compared to privacy which is about the intention of an organization to incorporate privacy-by-design throughout its ethos and digital architecture. He argued that WhatsApp had used encryption as a proxy for privacy. Data privacy is more than the security of personal messages in transit and should also encompass strong principles around a minimalist approach to the collection and processing of individuals’ metadata.

Privacy activists and journalists were eager to point out that ordinary WhatsApp users did not appreciate the value of their personal information – the metadata – that they routinely shared with WhatsApp, even if the content of their personal messages were encrypted. As we discussed in [Chapter 5](#), privacy journalists and activists drew attention to the fact that ‘you can get so much more data about a person from the metadata’. As Debarati from the NGO, Point of View explained, WhatsApp was ‘collecting metadata that still reveals a lot about you – when you’re sending messages, who you’re communicating with, and how often. Metadata can be used to establish these patterns and it makes surveillance much easier. So, encryption alone isn’t really meaningful as long as metadata is being collected.’

Consequently, privacy conscious participants such as the tech journalist, Aditi Agrawal was very careful not to generate metadata that could be analysed to make connections between her and the ‘sensitive people’ she interviewed for her work. This crucially meant using Signal over WhatsApp whenever possible, because of its more minimal data collection, though her preference was always to speak with sources in person to avoid any surveillance.

For many, the reason they used WhatsApp was not because it was end-to-end encrypted but because it was the most popular messaging app within their networks. Ipsita illustrated this sentiment when asked if she would continue to use WhatsApp if it removed end-to-end encryption from its service. She replied:

In all honesty, probably yes because that’s the pervasiveness of WhatsApp and I’m not using it for its brilliant safety; I’m using it because everybody is on it and uses it. Tomorrow if everybody moves to Signal, I will also move to Signal. So, I think I’m a typical case of herd mentality in that sense, I’m using what other people are using because I need to communicate with them.

The power of WhatsApp’s network effect exceeded its publicized commitment to privacy when it came to attracting and retaining users in India. This situation was more widely evidenced when, despite an initial spike in downloads of Signal and Telegram apps in 2021 following concerns

about WhatsApp's privacy policy, WhatsApp's user base ultimately remained unaffected ([Mihindukulasuriya, 2021](#)). Our research indicates that people used WhatsApp *despite* a lack of trust in WhatsApp's promise that end-to-end encryption protected their personal messaging and privacy.

State surveillance, leakage and evidence

Concerns about the limits of end-to-end encryption to keep messages private were not unfounded, for different reasons. In 2019 national media reported on the outcome of investigations by Citizen Lab with Amnesty International that spyware had been used to target the phones of 1400 human rights defenders around the world: 100 of those targeted were activists, journalists, electoral commission members and politicians of opposition parties based in India. Ronan Farrow's analysis for the *New York Times* revealed how WhatsApp first suspected that a vulnerability in its messaging platform was being exploited around May 2019 when Claudiu Dan Gheorghe, a software engineer, was alerted to an unusual signalling message. Signalling messages contain a code that is automatically sent by WhatsApp users to begin a call, but Gheorghe noticed that instead of starting the ringtone this code contained strange instructions for the recipient's phone. Further investigations by Facebook's security team in London indicated that the code was not a glitch but a sophisticated and precise 'exploit' of WhatsApp by an expert actor ([Farrow, 2022](#)).

All signs led back to the Israeli start up, the NSO Group and the work of Pegasus a cyberweapon with the potential to exploit a vulnerability in WhatsApp's architecture to sidestep end-to-end encryption and target messages on users' digital devices where they exist as decrypted content. Farrow interviewed the NSO's Vice President for product development who candidly explained 'You find the nooks and crannies enabling you to do something that the product designer didn't intend' ... 'Once in control the exploit loaded more software, allowing the attacker to extract data or activate a camera or a microphone. The entire process was "zero click" requiring no action from the phone's owner' (cited in [Farrow, 2022](#), np). The device owner does not even need to answer the video call for the vulnerability to be exploited and their phone infected with the malware. In 2019 WhatsApp filed a petition before the US's Supreme Court against the NSO Group which accused them of using its Pegasus spyware to compromise the phones of 1400 individuals over a two-week period.

When Amnesty International and Citizen Lab went public with their findings there was a sense of shock among journalists, civil society and activists. For those reporting on or seeking to hold the government to account, phone tapping was commonplace. But as Rohan Venkataramakrishnan, Associate Editor of Scroll, remarked: 'encrypted services like WhatsApp felt more

private’ and so ‘[t]he news of the WhatsApp hack was quite jarring’ (cited in [Asher-Schapiro, 2020](#), np). In an Opinion piece for the *Washington Post*, Will Cathcart argued that ‘[t]his should serve as a wake-up call for technology companies, governments and all Internet users. Tools that enable surveillance into our private lives are being abused, and the proliferation of this technology into the hands of irresponsible companies and governments puts us all at risk’ ([Cathcart, 2019](#), np).

While Cathcart does not name the Indian government directly, given the nature of who was targeted by Pegasus, there was a strong suspicion that the government had to be involved. In 2021 further allegations were made by the ‘Pegasus Project’ – an international consortium of 17 media organizations and Amnesty International – which leaked a list containing 50,000 phone numbers that were potential targets for spyware, 300 of whom were based in India. Subsequent forensic analysis revealed traces of the spyware on the devices of ten individuals including Prashant Kishor, a political strategist who had worked with many political parties and the editors in chief of The Wire (an online news portal), Siddharth Varadarajan and MK Venu. Other potential but unconfirmed targets included journalists and Supreme Court judges ([ANI, 2021](#); [The Wire Staff, 2021](#)).

The writ petitions warned about the spyware’s violation of citizens’ privacy and the implication of the attacks on the affected individuals’ networks: ‘Not only is the privacy of the Petitioners grossly violated, but also of the various sources that regularly and routinely converse with him and provide information.’ The use of spyware also presented a tangible risk of ‘state reprisal’ for people who ‘already come from marginalised communities or are otherwise already susceptible to state violence’. Moreover, there was a wider concern about the ‘chilling effect on freedom of speech and expression in India’. Meanwhile, the Government of India repeatedly denied the allegations and refuted the legitimacy of the claims. Rajendra Kumar, Additional Secretary in the Ministry of Electronics and Information Technology, argued the petitions were ‘based on conjecture’ and unsubstantiated media reports and that his primary objective was to convene a Committee of Experts ‘to dispel any wrong narrative spread by certain vested interests’ ([‘Manohar Lal Sharma v Union of India, Writ Petition \(Crl.\)’, 2021](#)).

Yet, there was no denying that in 2018 Narendra Modi and Benjamin Netanyahu, Israel’s Prime Minister, met in New Delhi where they publicly asserted a ‘new-era’ of cooperation particularly in ‘cyber-defence, security and science’ ([BBC, 2018](#)). As a *New York Times* report later revealed, Narendra Modi had signed a deal in 2017 between India and Israel for roughly \$2 billion which included the spyware tool, Pegasus as part of ‘a package of sophisticated weapons and intelligence gear’ ([The New York Times, 2022](#)). The 2018 budget for India’s National Security Council reportedly increased

ten-fold with most of the additional funding allocated to cybersecurity. Changes in the anti-terrorism law, the Unlawful Activities (Prevention) Act (UAPA), were also made to bring individuals, as well as organizations, under its mandate. After all, as Arundhati Roy (2021) wrote: ‘Organisations ... don’t have smartphones’.

In addition, Pegasus spyware is not especially affordable. In a media interview Shashi Tharoor, who was then a Congress MP and chair of a government committee tasked with investigating the alleged surveillance, suggested that such a purchase would have to be licensed high up in the government given that: ‘[i]t’s not the amount that could be authorized by a junior official’ (Asher-Schapiro, 2020). When asked for a statement, the NSO Group refuted allegations concerning phone hacking: ‘In the strongest possible terms, we dispute today’s allegations and will vigorously fight them. Our technology is not designed or licensed for use against human rights activists and journalists.’ Moreover, the group explained that: ‘We license our product only to vetted and legitimate government agencies’ (Outlook Web Bureau, 2019).

In his 2019 opinion piece for the Washington Post, Will Cathcart had voiced WhatsApp’s imperative to defend privacy and security and emphasized the technical and legal levers available to them: software code and the law.

The mobile phone is the primary computer for billions of people around the world. It is how we have our most private conversations and where we store our most sensitive information. Governments and companies need to do more to protect vulnerable groups and individuals from these attacks. WhatsApp will continue to do everything we can within our code, and within the courts of law, to help protect the privacy and security of our users everywhere. (Cathcart, 2019)

WhatsApp then took the NSO Group to court over its violation of US and California anti-hacking laws and for breaching WhatsApp’s terms of service by deploying Pegasus spyware on WhatsApp servers. In 2024 the legal case was concluded with the US court finding the NSO Group responsible and ordering them to ‘provide all relevant spyware’ for the period before and after the breaches were discovered, covering the period 29 April 2018 to 10 May 2020, and to supply WhatsApp with ‘the full functionality of the relevant spyware’ (The Wire Staff, 2024). At the time of writing, a court case is pending in India’s Supreme Court to decide whether there should be ‘an investigation into the Government of India’s alleged use of Pegasus spyware on journalists, activists and public officials’. In the meantime, reports have circulated that Indian government officials are concerned about the Pegasus ‘PR problem’ and seeking alternative spyware tools (M. Srivastava, 2023).

Pegasus was a different kind of ‘PR problem’ for WhatsApp. The use of Pegasus spyware to target phones via WhatsApp amounted to a major breach of the privacy of Indian citizens (as well as others globally) which provoked confusion and mistrust among civil society activists. To some extent, the detail of the Citizen Lab investigations was lost on some who took the Pegasus attacks as proof that encryption could ‘be broken’ as an NGO activist commented: ‘we are seeing with third party apps like the whole Pegasus thing, that you can actually access conversations on WhatsApp, right, so many journalists, politicians, etc. have been snooped on using third party apps. So how is it secure? End-to-end encryption can be broken.’ Aditi Agrawal reported to us how this meant that: ‘People had also kind of lost trust in WhatsApp then, because they thought their servers got hacked, and therefore everything got compromised.’ Aditi went on to argue that she thought the Pegasus revelations had proved more damaging to WhatsApp’s reputation as a secure messaging service than the backlash to its 2021 privacy policy update. Ironically, ‘WhatsApp wasn’t at fault’ in the case of Pegasus hacking devices, whereas it was at fault with regards to altering its data-sharing practices and amending its privacy policy agreements with users. ‘So, people, even jokingly will end up saying, ha, WhatsApp has Pegasus which is not true. Pegasus is not on WhatsApp. It’s on your device. WhatsApp is just one of the vectors to deliver it. But the Pegasus thing is what remains in people’s mind.’

The Pegasus story captured the attention of the media and India’s middle classes not only because it implicated WhatsApp but also because of the state’s alleged surveillance of high-profile journalists, intellectuals, politicians and activists, people like them. But, the routine state surveillance of caste, gendered, religious and racialized minorities in post-colonial India goes under the media radar. Everyday state surveillance is legitimized by and perpetuates historical and structural inequalities (Browne, 2015). Following the Indian government’s alleged use of Pegasus, its violent response to protests against the Citizenship (Amendment) Act (CAA) and National Register of Citizens (NRC) which discriminated against India’s Muslims by design, Srishti was doubtful about the existence of privacy in India, particularly for minoritized groups. Srishti worked for a government department and came from a privileged Hindu background. Reflecting on what she perceived as the widespread practice of data collection by the government and commodification of data by private companies she exhibited a sense of powerlessness or ‘digital resignation’ in the face of a government that can enter your home uninvited (Hargittai and Marwick, 2016).

It [privacy] used to [exist]. But not anymore, because the people of the ruling party, the right-wing, they can come to your space, they can just barge into your house, they can check what is in your fridge, and

you can get killed for it. So yeah, I think it [privacy] doesn't just exist anymore. Even if it does, it does for very selective people.

Like others we interviewed, Srishti was acutely aware that some people's communications were of more interest to the state than others; high-profile figures on the one hand and minoritized communities on the other.

Arman contextualized the importance he placed on privacy within a longer history of state surveillance in his Muslim majority neighbourhood, describing how he had grown up hearing stories about people being framed under spurious 'anti-national charges', whether that was on grounds of terrorism or something else. Arman explained that before smartphones, government informers would be 'planted' in his neighbourhood whereas today the state infiltrates social media and WhatsApp conversations to have 'people booked under UAPA' – the Unlawful Activities (Prevention) Act of the Indian Penal Code. Arman gave the example of the Bhima Koregaon case, where 16 human rights activists, artists and scholars were arrested in 2018 and charged with being part of a Maoist-linked conspiracy. He had read in the media that the state used Pegasus to infect activists' devices 'to compromise and frame them'. As he explained: 'That is why I say I don't want to be watched by anyone else, especially as a minority group, the Muslim minority.'

Arman argued that the relatively privileged, or at least well networked, position of those accused in the Bhima Koregaon case afforded them access to a fair trial, which was something he on the other hand, could not guarantee. This knowledge shaped his decision making about privacy.

I am not even talking about justice and as someone who comes from what you call a not so privileged economic background, I don't have that kind of access to power corridors, so I have to be a bit careful about what I do and ensure that nobody is watching me. ... Privacy is essentially a political concept, like everything is political, personal is political ... I would say that I am more concerned about privacy, as someone born into a minority community.

Arman went on to clarify that privacy was contextual, while he did not want his activities tracked, it also depended on who was collecting what data for what purpose. Like other minorities we spoke with, there was a tangible fear that the state was collecting information which, in India's exclusionary 'social atmosphere' could subsequently be used to criminalize them in some way. Arman further clarified: 'I don't have any issues if someone takes a picture unless that person is a policeman or something. That concerns me.'

Within this context of everyday state surveillance, particularly of India's minoritized communities, Arman also questioned the security of WhatsApp

chats in practice. Personal messages might be encrypted in transit, but they were nevertheless visible on devices:

I know that it [end-to-end encryption] is a process to keep the chats apart from people who are involved in the conversation, but it is pretty much useless because it only ensures privacy to the moving data which is on the WhatsApp server. It doesn't ensure privacy with regard to the storage on your phone. So, if a security vigil was involved what they cannot do is they cannot seek that chat on WhatsApp. What they can't do is provide access to the chats but if they are able to get access to your phone, the chats are there.

Others shared Arman's concern about how information could be captured and leaked directly from WhatsApp chats on people's devices and how, as Bahir commented, 'even on WhatsApp I feel very afraid of sharing anything which can turn into an issue'. Substantiating their concern, some referred to high-profile cases in which WhatsApp messages were circulated in the media and used as evidence in court cases. Raima referred to 'the Aryan Khan case' which drew on WhatsApp chats. As she remarked it was not the only incident, 'there have been similar incidents in which WhatsApp conversations were manipulated' and used 'against people in the communal violence as well in Delhi'.

Aryan Khan is the son of Shah Rukh Khan, one of India's most well-known Bollywood actors. In 2021 Aryan Khan was arrested on what the media dubbed a 'cruise ship drug case' by the Narcotics Control Bureau (NCB). Following the seizure of his phone, the NCB analysed Khan's WhatsApp group chats and claimed that they included 'group chats on drugs' and evidence that he was in touch with suppliers and had talked about the bulk purchase of drugs. An important dimension of the case concerned Aryan Khan's exchanges with another Bollywood actor, Ananya Panday who subsequently claimed that her reference to getting 'ganja' in the WhatsApp chat 'was meant as a joke' (Thaver and Modak, 2021). The high-profile incident undermined individuals' trust in WhatsApp's privacy claims, raising questions about the limits of encryption where messages can so easily be accessed and leaked from users' phones and used as evidence against them. As Raima went on to say: 'There has been enough evidence about how WhatsApp is problematic and can actually put you in situations where you can get trapped.' The networked nature of WhatsApp chats meant that the privacy of an individual's contacts was also compromised.

These narratives document how privacy was struggled over as an idea and a practice and in the process (re)constituted roles, relationships and power between individuals and machines/code, family, friends, civil society, the state and Big Tech (see Elwood and Leszczynski, 2011). People were concerned

with the limits of WhatsApp's security architecture to protect the privacy of everyone's messages and its relationship – unwittingly or otherwise – with a state government that has a long history of conducting surveillance on its citizens in the name of 'national security'. But as we intimated earlier in the chapter too, cultures of (digital) surveillance were also routine and mundane experiences, particularly for younger, often female and minoritized participants who described their efforts to protect their privacy from family and community members intent on policing socio-cultural norms concerning their bodies, boundaries and behaviour. That is the everyday work of privacy on and around WhatsApp that we turn to next.

Privacy work

'In India, securing your privacy is a mammoth task!' exclaimed Rinky in an interview conducted for this project. She was 20 years old and though she shared most things with her mother, who worked as a domestic help and encouraged her to continue studying, she also detailed the care she took to keep her photos and conversations on WhatsApp private from family members. Rinky's opinion that privacy was hard and required ongoing effort was also shared by Jamaal who explained how:

It's difficult to have anything private right now because everything is out there. It's the technology, but also in the everyday, it's about your movements and your phone, your parents asking where you are, all of that. But still we struggle and somehow keep ourselves private in whatever way is possible ... So yeah, privacy is mostly negotiating mundane activities at the same time as navigating this larger entity of the state and technology which you try to keep away from. I know it's not possible, and I know it's a privilege that not everyone has. Some people can't afford to have privacy.

The sentiments expressed by Rinky and Jamaal, and others too, embody the concept of 'privacy work' that captures the decision making and labour that people engage in to protect their privacy within a digitally networked world (Marwick, 2023). This section documents how participants variously engaged in 'privacy work' on and around WhatsApp and questions not just what privacy work entailed, but who and when participants guarded their privacy from and why. Though college and university students respectively, Rinky and Jamaal occupied different socio-economic backgrounds and gender, sexuality and religious positionalities. Like others interviewed for the project, their intimate global context informed how and why privacy mattered to them in India's patriarchal, Hindu nationalist and heteronormative societal landscape and in a global context shaped by Silicon Valley Big Tech. We

consider privacy work along three axes: privacy work, learning and literacy, privacy frustrations and cynicism, and how privacy work dialogues with the affective dimensions of dwelling in digital private spaces.

First, for many young single women, 'privacy work' was primarily articulated within the context of their family and community relationships and informed by their everyday experience of social surveillance. Before working as a health professional, Raima attended school in Meerut and lived with members of her extended family who were 'very conservative'. She contextualized the compulsion for her to engage in privacy work online by explaining how her extended family disapproved of her going to school in the first place and moreover that 'I did not take a *dupatta* [scarf] or I did not wear a burqa. And they [extended family] felt the social pressure that even if I am going, I should remain within the limits of the society.' The experience of family surveillance and anticipation of judgement within the wider community informed Raima's engagement with and on WhatsApp. She navigated her desire to represent her authentic self within her friendship circles, while protecting her image from the damaging judgments of her family members. As she explained: 'I was told that specific WhatsApp pictures were not okay' by her extended family. She went on to say that 'There have been incidents when people have gone to my home and questioned what kind of picture I have on WhatsApp. And then I have been scolded.' Raima rationalized this behaviour as an effort to 'shame' her and blamed her family's response on their ignorance of the internet which they understood to be a corrupting influence on women.

Consequently, Raima has learned ways to protect her WhatsApp presence. She was careful with which contacts saw her status as well as ensuring that her extended family could not see the 'last seen' messaging that appears alongside contacts. As for the image she used for her 'profile' photograph, she was conscious not to provoke an unwanted reaction, 'Even for my photos, I feel that I can't use those ones that I really like as my profile picture. So the profile pictures that I put are usually the ones where I appear very modest and like the image of an ideal woman.' Raima explained that sometimes she uses the photos *she* wants on display that reflects her mood and identity, 'but then I delete the phone numbers of my relatives and family members. So, they can't see [the photo] then. But this is not a very practical step.'

Like Raima, Rinky structured different spheres of digital privacy on WhatsApp among her family and friends by instituting different privacy practices. From taking care with the content she shared in different chats to selecting who could see her display photo, status and photographs. In addition, she kept her WhatsApp app in an 'app locker' on her phone, a hack she learned from her sister and subsequently researched on YouTube, so now no one in her family is aware of her secret 'locker'. Importantly, this meant her WhatsApp messages were secure from her brother who knew her

phone password and had a history of accessing it and sending messages from her WhatsApp to her contacts, including on one occasion, to her teacher which caused Rinky great embarrassment and shame.

Other research has discussed how social media produces ‘context collapse’ where ‘formerly distinct spatiotemporal arrangements, actual and imagined audiences, social norms, and information’ are brought together within ‘a common setting’ (Kini, Pathak-Shelat, and Jain, 2022, p 1575; see also Marwick and boyd, 2011). In the scenarios presented here, young people like Rinky and Raima deploy strategies such as ‘emotional filtering’ and technical affordances on WhatsApp as well as innovative social and technical hacks around WhatsApp. Such strategies delimited appropriate boundaries and resisted the collapse of their social worlds to protect their privacy, identity, reputation and therefore sense of freedom. Drawing on research with marginalized youth in India and Brazil on their intimate relationships and behaviours on Facebook, Arora and Scheiber are compelled ‘to view privacy not just as a social value and cultural practice but as a dynamic literacy’ (2017, p 415). Likewise, the privacy work articulated by Raima and Rinky encompasses sophisticated forms of privacy literacy, understood ‘as a socially situated process of learning that involves cognitive, digital, and social abilities, which enable learners to successfully engage in new communities across contexts that emerge in this contemporary age’ (Arora and Scheiber, 2017, p 419). Importantly, participants’ privacy stories typically expressed degrees of agency and privacy literacy in configuring WhatsApp’s technical features as well as engaging alternative sociodigital hacks and some sense of agency over their privacy within familial contexts.

The second observation is that privacy literacy was not always sufficient for realizing the feeling of privacy and safety in a geopolitical context shaped by state and Big Tech surveillance. While Raima had learned effective strategies for protecting her privacy from family members, she felt more powerless to predict what information Big Tech and the state might access about her and how that information could be used. Fearful that WhatsApp could be hacked, she chose not to discuss taboo subjects such as her relationships and ‘drinking’ and never sent ‘nudes’ or personal photos on WhatsApp, instead she just called people up to discuss more personal matters. She recognized the limits of her ‘technical expertise’ which meant she didn’t know ‘how easily people can access your data’ and because of this she always felt ‘anxious about using digital media’. Sharing growing ‘fresh’ concerns from the ‘religious or minority point of view’ that their safety was at risk, Raima’s brother had told her ‘not to circulate anything sensitive on WhatsApp’ because ‘of incidents when WhatsApp messages have been used to arrest somebody and put difficult charges on them’.

The experiences of Sabeena, who we introduced in Chapter 1, speak to Raima’s concerns too. Having witnessed her fellow students’ phones being tapped during the protests against the Citizenship Amendment Act,

she and her friends conscientiously protected their digital privacy from state surveillance. Sabeena described how she learned to moderate and mute her political opinions on WhatsApp after a particular incident. As she explained, feeling angered by the story of a young Kashmiri boy hit in the eye by an Indian army pellet, she had posted about the attack on her WhatsApp status. Soon after it was visible, '[T]here was this Kashmiri girl who said you won't be able to share all this or talk to people if you are charged under UAPA and put behind bars.' Heeding the girl's advice, Sabeena has since recognized that 'safety is a concern' on WhatsApp. Though she and her friends continued to use WhatsApp they did not trust that it was a private space and chose only to say what was already in the public domain, lest the police should seize their phones or screen shots of their messages enter wider circulation.

Ipsita articulated the level of personal responsibility that people like Raima, Sabeena and others felt to protect their digital privacy in the context of state surveillance and the profit motives of Big Tech. As she explained, the 'onus falls on me to protect my space and even if I am doing all the right things there is no guarantee that it will not be violated'.

I feel powerless because I don't know what I can do to protect my privacy beyond a certain point. Like I can do a two-factor authentication ... WhatsApp can assure me chats are encrypted and all you know but I don't trust these Silicon Valley people; they will read it when they want to, they will sell this data to the government for a profit when they have to and the government will buy it. So that is a thing I feel frustration about because I don't know what I can do to stop that. And a lot of the time there is hopelessness because some information you just have to give ... which is frustrating.

This scenario left Ipsita experiencing what she called 'digital privacy frustration' in the face of 'privacy cynicism' and the digital unknown (Draper et al, 2024).

In a reflective conversation with legal scholar, Dipika Jain, the question of privacy in digital age emerged as a concern, particularly in the context of potential state overreach. She observed:

One begins to wonder, could a private WhatsApp conversation with a partner, friend or colleagues later be interpreted or weaponised in a different context? In a system where digital infrastructure and Aadhaar are interlinked with banking and mobility, the boundaries between personal data and state access becomes deeply porous. One is concerned not only with the State but also with the global tech companies that mediate our digital lives.

Importantly, WhatsApp is interpreted within a wider landscape characterized by digital and privacy frustration informed by the post-colonial state's practices that do not have a robust history of protecting citizens' privacy, quite the opposite. Despite WhatsApp's marketing and media efforts to represent itself as the global protector of privacy, citizen-users remained cynical about it (and Silicon Valley's) privacy intentions.

Finally, privacy stories evoked the affective dimensions of dwelling in WhatsApp's 'digital living room' or 'digital *ghar*' (Gajjala, 2019). The privacy work required to protect participants' privacy speaks to feelings of potential jeopardy or insecurity that private spaces presented to some. For religious, gendered and political minorities, receiving and witnessing viral right-wing messaging within WhatsApp's subterranean spaces induced 'feelings of fear, anxiety, hurt and frustration' (Oza, Williams and Kamra, 2024). Nitya's account of her family WhatsApp group introduced in Chapter 4 revealed how private digital spaces were unevenly experienced. Despite Zuckerberg's techno-optimist vision, digital private spaces were not universally and positively experienced by all. As an idea and a practice WhatsApp's digital private spaces reproduced (patriarchal) power and privilege. In the case of Nitya, dwelling in the private WhatsApp group left her feeling offended, frustrated and alienated by the circulation of Hindu right-wing content, and the perceived limits of voicing her dissent or contributing a diverse opinion. While the privacy of the group provided a space for her senior relatives to espouse extreme views that produced or reinforced their feelings of intimacy and connection, it did not afford Nitya the freedom to be herself and express her political opinions (see Chakrabarti, Stengel and Solanki, 2018). Intent on protecting her personal wellbeing, Nitya eventually left the extended family WhatsApp group, with her mother's implicit support.

While Nitya exited the private digital space, other minoritized citizens interviewed for the project instead modified their participation within diverse private groups by muting, moderating or filtering their voice to mitigate against previously hostile responses from other 'mainstream' members (see Chapter 4). Despite engaging in 'privacy work', new entanglements of the social and political in the 'digital living room' served to reinforce existing power hierarchies between genders, religions and generations and elide the role of the political within 'home-like' spaces while simultaneously strengthening a Hindu majoritarian state ideology from within. WhatsApp's private enclosures have therefore become domesticated and mobilized in ways that serve to discipline sociopolitical relations in everyday life and draw boundaries around who is included and excluded, not only within the 'digital living room' but also within a Hindu majoritarian nation state. WhatsApp's digital private spaces are not universally inclusive, domestic-like or democratic spaces rather they can also cultivate affective feelings of exclusion, contributing to the un-making of home and the un-making of democracy.

Conclusion

Recently overwhelmed by new levels of spam and adverts on WhatsApp, Namita had moved her communications to Signal and Telegram. Shifting platforms had prompted her to reflect with some irony on how ‘our privacy is kind of dependent suddenly on individuals and their interests’ who are elsewhere, in Silicon Valley or Europe, and always male. The privacy stories we shared in this chapter attest to situated ways in which privacy is a social and material relationship variously navigated through simultaneously intimate and global lives. The irony is that the digital private lives of WhatsApp users in New Delhi are designed by ‘architects’ in Silicon Valley. Removed from the situated concerns of their everyday lives, the decisions of WhatsApp’s software engineers have far-reaching implications for how digital space is ‘lived’. This is the intimate geopolitics of digital privacy.

Within a context of community and state surveillance and global data capitalism, privacy resonated and mattered to differing degrees within people’s lives. The gendered and political minorities we interviewed for the project were generally most animated about the value of privacy often in the context of the risks of privacy violations. While younger women prioritized the importance of privacy work within their home and family lives, Muslim men and women most feared the surveillance of the state and its collaboration with Big Tech in ways that might profile, target and incriminate them unfairly.

Despite Mark Zuckerberg’s techno-optimist vision that digital private spaces were the future and safe from hackers, criminals and rogue governments, WhatsApp was not universally perceived and experienced as a digital private space that provided sanctuary and security or supported democratic practices and principles. But WhatsApp did enable degrees of privacy. To some extent, people believed that through their diligent privacy work – configuring WhatsApp’s privacy settings or using informal hacks – they had some control over their privacy from family and other community members. Meanwhile WhatsApp simultaneously afforded a digital private escape away from ‘in person’ interactions. But dwelling *in* WhatsApp’s digital private spaces as a gendered, religious and/or political minority could present fresh challenges. Participants shared their experiences of learning how to exit groups or mute or moderate opinions while tolerating the discriminatory and exclusionary messaging that circulated in WhatsApp’s ‘deep addresses’.

By contrast, participants expressed feelings of digital resignation, privacy cynicism and digital privacy frustration when faced with the (im)possibility of navigating their digital privacy from the state, Meta and Big Tech more generally. As a ‘privacy thing’ the very fact of end-to-end encryption appeared less materially important, misunderstood and distrusted. More important

was the feeling of intimacy created through the presence of friends, family and close networks. What attracted and maintained people's attention on WhatsApp was the suck of its network effect, a crucial resource that Meta actively matured before turning WhatsApp into a meaningful business, as we turn to in the [next chapter](#).

WhatsApp (in) Business

Turning WhatsApp into an app for business

Meta's introduction of a new app, WhatsApp Business and the WhatsApp Business Platform, has gradually changed how people's WhatsApp inboxes look. For most Indians who use WhatsApp, the app no longer contains only messages from their friends, family and acquaintances. WhatsApp inboxes are also filled with messages from the shops, restaurants and online stores that people have given their phone numbers to while shopping or using a service. It is now a common practice for a business to ask for one's phone number not only when processing payments online but also when paying bills in person at a shop or restaurant. Businesses then use their database of phone numbers to send messages through Meta's WhatsApp Business Platform. Harjot Kaur, an IT manager based in New Delhi, was one of our respondents who received messages from many businesses. For her, the barrage of messages from businesses meant that WhatsApp had stopped being a space she considered private. As she told us:

I do get [WhatsApp] messages from Amazon. ... If you have ordered something from Amazon or Swiggy [a food delivery app] then banks also reach out, you know, with their offers and stuff. But coming to small scale businesses ... I have bought a television and stuff from a local shop owner and then that person ended up adding me ... in their list and they keep on sending me offers. ... I think spam is also equally increasing ... I don't think it's [WhatsApp] a private space.

From big companies such as Amazon to food delivery platforms and local electronics shops, businesses use WhatsApp to send offers, display products and provide customer service while also apparently sharing their database of customer phone numbers with other third parties, in this case, banks. Medium and large size businesses use the WhatsApp Business Platform to message customers at scale – for instance updating on an order placed or

sending cinema tickets or flight boarding passes – to drive marketing support and sales outcomes and personalize promotions. WhatsApp charges businesses a fee for the service dependent on country and message volume (WhatsApp, 2025c). Users like Harjot shared that receiving WhatsApp messages from big businesses felt like an unsolicited invasion of their WhatsApp inbox and an erosion of digital privacy.

In addition to the paid WhatsApp Business Platform, Meta has a free-to-download WhatsApp Business app. Shubhojit Sen, who runs a small business supplying speciality Bengali sweets in the national capital region of Delhi, told us:

I have WhatsApp Business. ... I have a proper catalog there. Like everything with the photo, with the description, with the size, with pricing. If anyone wants to know [what I sell]. ... [A]nother thing is, WhatsApp Business has a very interesting feature where I can send ads right away from WhatsApp ... that has given me a very interesting result. I will give you the ballpark idea about how it actually works. I have spent around ₹300 [equivalent to £3] for two days of ad campaigning. I kept my radius at 5 km ... I received quite a good level of queries [as a result].

The WhatsApp Business app helps Shubhojit communicate with his potential customers through WhatsApp messages and the app's special features. Business owners can create 'catalogs' (we use the American spelling because the WhatsApp Business app uses it) to upload photos of their products and pay a small fee to create ads to attract potential customers. The fee for one ad in India in March 2025 was ₹87, equivalent to £0.80. Small businesses are encouraged to use WhatsApp Pay for in-app payments, to display 'catalogs' of their products and communicate directly with customers.

The WhatsApp Business website advertises a third product, ads that Click-to-WhatsApp. When ads are clicked, they open a WhatsApp chat with the advertising business for customers to initiate a conversation. Uber and Amazon represent some of WhatsApp's largest business partners in India. Click-to-WhatsApp Ads monetize WhatsApp's growth by leveraging Meta's existing ad platforms. Businesses can add a 'call to action' button on their Facebook and Instagram ads, that when clicked, will lead the potential customer to a WhatsApp chat with that business (WhatsApp, 2025b). This feature also enables connections across the different integrated Meta platforms, enabling Meta to collect user information. As WhatsApp head Will Cathcart pointed out,

[W]e do have a lot of businesses on WhatsApp who want to advertise on Facebook or on Instagram, and instead of having people who see

those ads go to a website, have them message the business on WhatsApp ... So, they run these ads on Facebook where the button says, 'Message me on WhatsApp.' You only see that ad if you have WhatsApp on your phone, and if you're clicking those ads on Facebook, obviously that changes the ads that you see on Facebook. (Chundru, 2021)

All three products are revenue generating means for Meta through WhatsApp. They represent a significant departure from WhatsApp as a tool for personal private messaging.

As discussed in [Chapter 2](#), WhatsApp Business was piloted in 2018 as part of Facebook's efforts to monetize WhatsApp and make it 'a meaningful business in its own right'. Now an integral part of what Meta calls its 'family of apps' with over 1.5 billion users worldwide, WhatsApp Business has its largest number of users in India. At the first WhatsApp Business summit in Brazil in 2022, Zuckerberg touted WhatsApp Business as a dedicated app to support and help businesses which were already organically using the ordinary WhatsApp chat ([YouTube, 2022](#)). Zuckerberg and Meta present WhatsApp Business as a social and economic utility, especially for small businesses who can download the app or create 'catalogs' for free. The WhatsApp Business website publicizes the 'success stories' of businesses of all sizes that have used WhatsApp Business app, platform, and/or clickable ads to grow. The success stories conceal the shifting terms of WhatsApp's data and privacy policy we detailed in [Chapter 5](#), in order to implement WhatsApp Business.

In India, WhatsApp Business was piloted within a context where people were already informally mobilizing WhatsApp for their business needs. In 2018, Chris Daniels, the then WhatsApp Vice President, indicated in an interview that 50 million businesses in India were already using WhatsApp for their work. Chris Daniels' pitch was that WhatsApp wanted to build new tools to support these businesses and ultimately drive economic growth in India ([Singh, 2018b](#)). As this book shows, WhatsApp lands differently in different contexts. In this chapter we focus on Meta's discursive and technical construction of WhatsApp Business in dialogue with users' experiences in India. We argue that the design and domestication of WhatsApp Business has depended upon the erosion of WhatsApp's data privacy promise on paper and in practice in four important ways.

First, as the 2021 privacy policy update communicated ([Chapter 5](#)), users' data and in some cases, messages are shared with WhatsApp Business and third parties once they interact with a WhatsApp Business account. Second, the integration of WhatsApp and WhatsApp Business means that users' affective experience of WhatsApp as a more intimate, private digital space is undermined by the overwhelming amount of business advertising and spam communications they now receive on their WhatsApp. As shown in the [previous chapter](#), while users might not always trust the security of

WhatsApp, they typically value it as a digital space they share with more intimate and familiar contacts and over which they have some control. Third, the introduction of WhatsApp Business in India further normalizes a shift towards sharing personal data to access social and economic life which Aadhaar ushered in. In this case, as more and more businesses operate through WhatsApp Business, one's phone number is now routinely requested at shop tills, cinemas and restaurants and sharing it has become essential for identification and inclusion within economic life. Finally, Meta's techno-optimist narratives promote WhatsApp Business as inevitable for and as a social and economic good that will power India's development. These discourses simultaneously sideline WhatsApp's earlier privacy promise and implicitly position greater data sharing between WhatsApp, Meta and Third parties as a necessary trade-off for India's development.

Each section of this chapter discusses a different aspect of the erosion of privacy due to WhatsApp Business. We draw on discourse analysis of WhatsApp Business material available on its website and interviews with small and medium-size business owners as well as ordinary users of WhatsApp and WhatsApp Business. The second section illustrates how WhatsApp's new data relations erode privacy. The erosion of privacy argument is further developed in the third section through interviews with WhatsApp users in India, who frequently receive a large number of WhatsApp messages from businesses and no longer see WhatsApp as a digital private space. We also examine here how the rise of WhatsApp Business has fed into the production of the phone number as a public and essential object for transactions in everyday life, further eroding people's privacy. The fourth section discusses the entanglement of Meta, which pushes WhatsApp Business as a socio-economic utility, with the Indian government, and the implications for privacy therein. The fifth section analyses interviews with small business owners who used WhatsApp Business and documents how any concerns over privacy are sidelined by the convenience of WhatsApp (in) Business.

Erosion of data privacy

Given a strong legacy commitment not to place targeted advertisements on WhatsApp, the challenge for Meta has always been how to monetize WhatsApp without fundamentally changing the design ethos of the original WhatsApp product. In June 2025, even as WhatsApp formally announced the introduction of ads, Will Cathcart told users that their privacy was still intact (Lochab, 2025). It could be argued that WhatsApp Business provides a work around for Meta to access and monetize WhatsApp users' attention while leaving the original WhatsApp infrastructure intact. As discussed in Chapter 2, Zuckerberg's priority was to grow WhatsApp's user base and *then* transform it into a meaningful business. This growth model ultimately led

to the testing of WhatsApp Business and WhatsApp Pay in 2018 in India and Brazil. Subsequently, a privacy policy update in 2021 laid the ground for expanding the platform's data relations with businesses beyond Facebook (see [Chapter 5](#)). Users were asked to 'Agree' to the new terms of service by January 2021 or lose access to WhatsApp. The 2021 update undermined user trust in WhatsApp and the backlash by the media and the Indian government on grounds of its citizens' privacy altered the perception of WhatsApp as a space where one's privacy is protected (see [Chapter 5](#)). Responding to the public backlash Meta created ad campaigns that stressed to users how their privacy was operationalized through end-to-end encryption and centred the feeling of privacy in order to rebuild users' trust in its product (see [Chapter 6](#)). As we argue throughout this book, Meta narrates, designs and performs the idea of privacy in the pursuit of profit.

WhatsApp Business marks a departure from WhatsApp's original commitment to user privacy. We argue that user privacy is both overtly and subtly undermined through Meta's three revenue generating products: WhatsApp Business app, WhatsApp Business Platform and Click-to-WhatsApp ads. WhatsApp Business presents users with more complicated privacy features where it is hard to figure out how to turn on privacy settings. One major concern for users is whether their privacy would be compromised by Meta when they use the ordinary WhatsApp app to communicate with a business or individual who is using the WhatsApp Business app or platform. The WhatsApp Business website's 'Business Privacy' page states, 'Our mission is to securely connect businesses of all sizes with their customers' ([WhatsApp, 2025e](#)).

'Secure' is the keyword here. When a user of the ordinary WhatsApp app gets a message from a business, they are shown a message which says, 'This business uses a secure service from Meta to manage this chat'. If one taps on this option, one is given information about how one can block a business easily to control who one chats with. WhatsApp Business does give a prompt to block or accept messaging with a business when they message someone for the first time. On the other hand, if two users are connecting through the ordinary WhatsApp app, the message that appears on the screen states that 'Messages and calls are end-to-end encrypted. No one outside of this chat, not even WhatsApp, can read or listen to them.'

This difference between 'secure' and 'end-to-end encrypted' messaging has implications for privacy. Meta claims on its 'Business Privacy' web pages that (secure) chats between customers and businesses follow an 'encryption protocol', but it collects 'certain information' from these chats. Message and call content is not shared with Meta, but the 'information helps businesses send you relevant messages and improve Meta ads' ([WhatsApp, 2025f](#)). Moreover, when businesses choose additional 'optional services' such as storing messages with Meta or using Meta's AI assistant, user data from

WhatsApp Business apps is available to Meta. When these businesses work with Meta's 'business solution partners', they also share the data with these third parties. Overall, metadata such as a user's phone number, transaction data, interaction data, device information and IP address are collected to show a user ads on Facebook and Instagram without using data from messages. However, when businesses use Meta AI on WhatsApp Business to help them respond to customer messages, then Meta will 'receive these chats to improve its AI quality and generate message responses' ([WhatsApp, 2025f](#)). In short, there are ways Meta can access chats through AI when users communicate with a WhatsApp Business account.

A report by ProPublica published in 2021 argues that the introduction and integration of WhatsApp Business has resulted in 'a confusing two-tiered privacy system within the same app where the protections of end-to-end encryption are further eroded when WhatsApp users employ the service to communicate with businesses' ([Elkind, Gillum and Silverman, 2021](#)). Meta's claims to being committed to users' privacy are therefore questionable in the hierarchy of privacy that they have now established. Meta capitalized on WhatsApp's network effect underpinned by its popularity and the trust people have in the app to build a new app that would generate a profit (see [De, 2024](#)). But in doing so, WhatsApp's practical commitment to data privacy has been eroded.

The Pro-publica report also draws on a Meta marketing document from 2020 to evidence 'WhatsApp's diverging imperatives'. Whereas WhatsApp's brand identity centres the ability to 'message privately', the marketing presentation states that 'privacy will remain important'. But it also conveys what seems to be a more urgent mission: the need to 'open the aperture of the brand to encompass our future business objectives' ([Elkind, Gillum and Silverman, 2021](#)).

The importance of privacy is not promoted on the WhatsApp Business website apart from directing users to the privacy policy on a separate 'Business Privacy' page. The discursive shift from privacy to profit can be traced through Facebook/Meta's quarterly earning calls. In Facebook's Quarter 3 Earnings call for 2018 Zuckerberg referred to the recent launch of WhatsApp Business and emphasized the importance of maintaining the app's commitment to simplicity and privacy:

When it comes to messaging, we have an opportunity to help people and businesses connect in ways that are valuable for both. On Messenger, over 10 billion messages are sent between people and businesses every month. It's still early, but we're exploring how we can help advertisers reach people in Messenger through Sponsored Messages and Inbox Ads. For WhatsApp, we're growing our business ecosystem, starting with the WhatsApp Business app on Android.

In August we launched the WhatsApp Business API to help larger companies send useful information such as boarding passes or delivery confirmations. This paid messaging model will ensure that companies are selective about what they send and don't clutter people's chats. As always, people will be able to block any business they want with one tap. As we build a business on WhatsApp, we're determined to maintain the simple, private user experience that people love. ([Facebook, 2018b](#))

Clearly, the 'private user experience' was very much a part of WhatsApp Business discussions in the early days. But in 2020, discussions concerning WhatsApp Business in Meta's meetings shifted towards a focus on revenue generation. In the 2021 Quarter 4 earnings transcript, one finds that the company saw the most 'momentum' in its business app and began to expand it to partner with companies like Uber and JioMart (in India) to enable taxi bookings and grocery delivery through a WhatsApp chat ([Facebook, 2021](#)). After 2022, reports indicate that WhatsApp Business drove all the increases in Meta's non-ad revenue from what the earnings transcripts refer to as the 'Family of Apps'. For example, the Quarter 4 earnings transcript mentions that the WhatsApp Business Platform drove revenue growth by 85 per cent in Quarter 1 of 2024 ([Meta, 2024](#)). WhatsApp was finally contributing to Meta's earnings.

This growth was enabled by the growing popularity of WhatsApp Business in the global south. Meta's own studies show that 90 per cent of its users in India, Brazil and Indonesia chat with a business at least once a week ([Lapowsky, 2024](#)). Big businesses which operate in markets where WhatsApp is used for all aspects of life choose WhatsApp Business Platform. For example, one of the 'success stories' listed on the WhatsApp Business website is that of Domino's Pizza Indonesia. An American pizza chain, Domino's operates across the world and found WhatsApp Business particularly helpful for increasing sales and retaining customers in Indonesia ([WhatsApp, 2025d](#)). In countries like Indonesia, aside from the WhatsApp Business Platform, the WhatsApp Business app has over 200 million users among small and medium businesses ([Lapowsky, 2024](#)).

The connection between WhatsApp Business' expansion into major markets in the global south and the erosion of privacy protections is hard to ignore. The initial roll out of WhatsApp Business has depended on comparatively weaker national regulatory contexts, such as in India and Brazil, as we discussed in [Chapter 3](#) (also see [Arora, 2019a](#)). The updates to the privacy policy in 2021 that reduced users' privacy protections exploited globally uneven data and privacy regulatory landscape. The success of WhatsApp Business relies on Meta operating two paradoxical strategies. On the one hand, it promotes privacy as the unique selling point for WhatsApp. And on the other hand, it designs and promotes WhatsApp Business and

a business model that depends on weaker data privacy protections enabled by the absence of stronger data regulation policies in different territories.

Shifting user privacy experiences

In addition to altering WhatsApp's data relations, the WhatsApp Business model also undermines people's experience of WhatsApp as a private digital space for personal messaging. The flood of messages that users like Harjot experience from WhatsApp Business accounts and platform, changes their perception of WhatsApp as a messaging app for personal communication. We discuss how the perception or feeling of privacy is eroded in two ways: through users becoming overloaded with messages from WhatsApp Business accounts; and people's phone numbers becoming a public object due to the increasing reliance of businesses to communicate and offer customer service through the WhatsApp Business Platform.

Dealing with business messages

Seema Singh, an academic based in New Delhi, woke up at 9 am and checked WhatsApp on her phone. She had received promotional messages from two clothing shops, membership offers from a chain of gyms and a message from Amazon.in about some items she had ordered on the website. Only after scrolling down for a while passed other business notifications did she find a message from her mother. She was irritated that her WhatsApp had been overtaken by impersonal messages. Like Seema, many Indians feel that their WhatsApp gets overloaded with impersonal messages, and their WhatsApp inbox becomes a less private space as compared to before when it was a means to communicate with friends, family and acquaintances through groups and one-on-one messaging.

When Seema sees messages from businesses, she often exercises the option to block the business. This option appears on top of a chat window users share with a WhatsApp Business account. To show that they care about privacy, Meta gives its users a veneer of 'privacy and control' by simply stating that 'WhatsApp always makes it clear to people when they are chatting with a business, and they can block a business at any time' (WhatsApp, 2025e). On the FAQs page for WhatsApp Business, one can see the following text:

You're in control

WhatsApp wants to make sure you know what's happening with your messages. If you don't want to receive messages from a person or business, you can always:

- Block them directly from the chat
- Delete them from your contact list

We want to make sure you understand how your messages are being handled. We also want to ensure you have the options you need to make the right decisions for you. (WhatsApp, 2025f)

The idea that the ‘control’ is in the hands of users is underpinned by the notion of the liberal political subject who has responsibility for managing their own privacy, as we have detailed in [Chapter 4](#). The choice available is to block or delete an account they do not want to receive messages from. Yet, it is Meta’s introduction of the WhatsApp Business Platform that means users’ WhatsApp inboxes are being filled with unwanted messages in the first place. The shift of responsibility from Meta to the user erodes privacy, even as Meta performs privacy through its privacy policies, marketing campaigns and privacy features.

An erosion of privacy for those who communicate with WhatsApp Business accounts also happens when businesses choose to share user information with Meta. But the WhatsApp Business website tells its customers that they have choice and control even then: ‘If businesses choose to share information with Meta, users have the option to review their Ad settings and choose whether Meta can show them ads on Facebook and Instagram based on their activity from Ad partners’ (WhatsApp, 2025f). Users rarely understand how to navigate the maze of settings required to protect their privacy, so information is shared with Meta by default. Our interviewees mostly used the ‘block business’ option but little more. Again, while blocking businesses is straightforward and many users do exercise this option, it again puts the onus on the user to take ‘control’ and the burden of additional labour to maintain their privacy.

Among those we spoke with, there was a sense of discomfort that WhatsApp was becoming an impersonal app where users have no control over who contacts them. For users of the ordinary WhatsApp app, interactions with businesses (including blocking) and social interactions with family and friends take place on the same app (Johns, Matamoros-Fernández and Baulch, 2023, p 148). This alters how they view this private digital space, as our respondents in India told us. Just as Harjot stated that WhatsApp is no longer a private space for her, Vijay Singh, a master’s student based in Delhi, indicated his annoyance at receiving several messages from any business he has shopped at or registered with. He earlier considered WhatsApp to be a very private space where he would only interact with friends and told us: ‘Sometimes, it can be irritating. Because we don’t need such things all the time ... the messages are popping up all the time.’ However, unlike Harjot, he didn’t block businesses that messaged him, not wishing to miss out on potentially useful offers and promotions. Whenever he would get ‘irritated’, he would mute a business on his WhatsApp rather than blocking it. Harjot and Vijay might interpret what Meta calls ‘control’ in different ways, but the feeling of being spammed in what they considered a private intimate space is common.

Like Vijay, Akshay Dwivedi, a software developer based in Delhi conceded that customer service on WhatsApp is a ‘good thing’. He acknowledged that his WhatsApp inbox has changed, and more shops ask for his number when he goes shopping, but he still considered it to be a private space as he primarily uses WhatsApp for conversations with friends. He considers end-to-end encryption, as well as the ability to use WhatsApp features such as disappearing messages, as assurances that his conversations are private. He chose to limit all personal messaging to WhatsApp rather than Instagram due to WhatsApp’s end-to-end encryption feature. He had never read WhatsApp’s privacy policy and continued to see it as more secure and private compared to other apps.

Ravi Mann saw business messages on WhatsApp as an invasion of his private space:

They [WhatsApp] are trying to enter in my personal space by sending me a promotional message because they know that many people use WhatsApp. So if they send me things on WhatsApp, people have a human tendency generally they see the messages on WhatsApp. So I think that’s the agenda, but personally I would say that if someone has sent me a promotion message I just select the delete option without sometimes having read the message at all.

Blocking business accounts and deleting business messages are some of the ways users handle the spam. Users’ differing responses show that they care about privacy to varying degrees and use different privacy-related affordances to shape how they use WhatsApp Business.

Meta’s celebration of WhatsApp Business is in tension with how some people perceive the intrusion of business messages as annoying and experience WhatsApp as a less private digital space. When one’s WhatsApp *feels* less private and intimate it becomes normalized to receive messages from business accounts and impossible to decline further business requests to share personal phone numbers. Despite the introduction of new privacy features that promise individuals greater choice and control, the complexity and demands that such ‘privacy work’ places on individuals means that data often flows to WhatsApp (Meta and third parties) by default. The introduction of the WhatsApp Business Platform and related apps has thus fundamentally eroded the nature of WhatsApp’s private digital spaces, despite Meta’s performative privacy and public assurances otherwise

The phone number as a public object

WhatsApp Business has also made it more acceptable to ask for phone numbers. The practice of asking for phone numbers by the state and by businesses has a

kind of ubiquity in India that it doesn't in Europe and North America. The Indian government's JAM (Jan Dhan, Aadhar and Mobile number) trinity initiative to transfer cash benefits directly to the intended beneficiary requires a mobile phone number to be linked to Aadhaar and a person's bank account. And with WhatsApp Business, there is an expectation to share one's phone number when asked, even if it is someone one has just met. Cashiers at shop tills, workers at cinemas, salons, restaurants and cafes routinely ask for phone numbers with the expectation that it will be given. These days, refusing not to provide your phone number, even if it is to protect your privacy, can make it harder to buy things or access services. At a shop till, if you say that you don't want to provide your number, some cashiers might accept the request while many others will have to refuse, some citing that a phone number is essential for the billing software. In some spaces, providing a phone number has become a quasi requirement to participate as an economic citizen. Hari from the south Indian state of Kerala shared how he begun refusing to give his phone number to cashiers and was met with disbelief:

That is a surprise for them because normally people don't say 'no'. People easily give their phone number, they don't think so much at that time. Only after some realization happens then they think about it. It is a surprise for them when people say no, but we have to stick to our point.

Seema Singh, a researcher based in Delhi told us that it took her some time to realize that she could refuse to give her phone number:

Earlier, I didn't even think I had a choice. They have asked so I have to give [my number]. It never struck me that I could ask ... 'is it necessary to give my number' It is not! I never even thought about not sharing my number until I saw my husband doing it. He told me that sometimes your information gets leaked or is sold to third parties which can be a security risk ... and that is why I have started to categorically say 'no'.

Seema was also prompted to say 'no' to sharing her phone number after she received WhatsApp messages saying 'hello' from unknown numbers which were not business accounts. Her fear was that her phone number and data were being passed on to other third parties by the businesses she had interacted with.

Harjot came to similar conclusions about her data being shared and made a distinction between local small businesses and big stores, where it's the latter who are more likely to pass on the phone number:

I think generalizing would be difficult. It depends. I think a lot of small vendors don't do it ... Like, [it] could be a mall thing, you know,

where there are a lot of shops, right? I would say a mall person, or someone who is not directly invested, they might be playing around with the contacts they have.

Since big stores dealt with customers more impersonally than local shops, Harjot's solution was to provide a wrong phone number to big stores. Doing so protected her from spam calls, which many have been receiving increasingly on WhatsApp accounts in India as Harjot reflected:

I think spam is also equally increasing. I think, I read about getting random calls from people for money and all that. I've been getting random video calls ... I never pick up from a strange contact. I know nobody can receive a call, whether it's a regular or WhatsApp, but I was getting a lot of WhatsApp calls also. So there was a surge in between ... I've heard that people who were picking up the calls, they were getting logged into some spam call and then ... So, yeah, I think everyone is using WhatsApp for that purpose.

The 'purpose' for using WhatsApp that she refers to is cold calling by businesses or scam calls where people are asked to pay money on false pretexts. For instance, there were several cases in 2023 where people got calls from scammers posing as police officers who told people that they have been implicated in a case and must transfer money to get out of the allegations. After being asked by the Indian government to act, WhatsApp introduced a new feature in its privacy settings where users could select a 'silence unknown caller' option to automatically block WhatsApp calls from scammers and unknown numbers ([Economic Times, 2023](#)). In 2024, there were cases of scammers making video calls and taking control of people's smartphones after asking them to share their screens, and the Indian government sent a notice to WhatsApp once again ([Times of India, 2024](#)).

However, when people want to block messages from businesses or potential spammers they don't just rely on WhatsApp's privacy settings. They also take actions like giving out a wrong phone number or refusing to give their number to shops and businesses but this sometimes produced friction or came at the cost of accessing services. Lipika, one of the authors of this book, had the following exchange when buying cinema tickets in a town in Haryana, close to the state's northern border with Delhi.

Lipika:	Can I have two tickets please?
Cashier:	Your WhatsApp number please.
Lipika:	Why do you need my WhatsApp number?
Cashier:	To send the tickets.
Lipika:	Can you not print them out on paper?

Cashier: No, they have to be sent digitally. Either you book them online or give me your WhatsApp number.

Lipika complied and gave her number, promptly received the tickets which a security guard scanned at the cinema door and let her in. She later thought, ‘What if someone does not have WhatsApp? Why is WhatsApp the default and perhaps the only way of getting cinema tickets?’ Feeling uneasy, she decided to question the cashier the next time she went to the same cinema. This time the conversation went as follows:

Lipika: Two tickets for the 4pm show of Merry Christmas [a Bollywood film], please.
 Cashier: Your WhatsApp number?
 Lipika: I don’t want to give it.
 Cashier: For the tickets, you have to.
 Lipika: What if I say I don’t have WhatsApp? Or, that I don’t have a smartphone?
 Cashier: You can get the tickets through a text message then.
 Lipika: You are sure you can’t just print the tickets?
 Cashier: No, Ma’am
 Lipika: Okay, here is the number [not wanting to miss the opening scene of the thriller movie]

Lipika stood at the door with her phone in hand, but the text message did not arrive. She grew very impatient and fought her way in, sat down and started to watch the film. The text message arrived 40 minutes after the film begun.

During the intermission, the manager approached Lipika saying, ‘Please do give the security guard your phone number before you go in, even if you did not receive the tickets on your phone right away.’ Lipika answered that she cannot give her phone number everywhere and that cashiers should not insist on people sharing their WhatsApp numbers. The manager replied that he understood but according to the new rules, cinema tickets could only be issued digitally.

Lipika’s experience at the cinema is an example of how the telephone number is socialized as a public object of identification within India’s socio-cultural context. Someone’s phone number is personal data that can be used to identify a specific individual and is not public property. While WhatsApp and Meta are not responsible for policies evolved by cinema chains and their managers, WhatsApp Business’ ubiquity creates situations where it is impossible for customers to make transactions, whether online or digitally, without providing their phone number. By giving out their number, they implicitly agree to receiving messages from a WhatsApp

Business Platform account. Resisting or being unable to meet such requests impacts an individual's ability to participate in economic life. Moreover, users' informational privacy is eroded by the expectation that their phone number is public property. The embedding of WhatsApp Business serves as an example of how Meta and WhatsApp are reconfiguring boundaries of private and public data, perhaps in unanticipated ways.

WhatsApp (in) business, government and corporate power

Modi and WhatsApp Business

Indians do not just receive unsolicited messages on WhatsApp from businesses but occasionally also from their own Prime Minister. Between 14 and 17 March 2024, many citizens received a WhatsApp message from an account that was named *Viksit Bharat Sampark* (Developed India Communication). The message, accompanied by the words that 'this business uses a secure service from Meta', had an attachment in the form of a letter from Prime Minister Modi where he asked citizens to give suggestions on shaping a *Viksit Bharat* (Developed India). The letter detailed the 'transformative efforts' and 'historic and major decisions' that his government had already taken. In the spirit of 'public participation', he asked people to support the 'resolve of building a Viksit Bharat'. The letter and the WhatsApp text accompanying the pdf of the letter were both in English and Hindi. The text requested people to share feedback and suggestions but did not specify how to do so. Were they expected to reply to the WhatsApp message? Was Modi using WhatsApp so that there could be a two-way communication between him and the citizens? After all, he had already set up his own WhatsApp channel in 2023, so he was aware of WhatsApp's potential (see [Chapter 3](#)). Only this time, he had used the WhatsApp Business Platform since it allowed senders to reach a large number of recipients at one time.

It was no coincidence that the letter was sent soon after the elections were announced. Some pointed out that it was in violation of the model code of conduct, which kicks in as soon as elections are declared and requires the government to stop announcing any new welfare schemes that would give the ruling party an unfair advantage in the campaign. Here, the ruling political party was Modi's BJP. After complaints from opposition political parties, the Election Commission prohibited bulk WhatsApp messages during the election period and especially instructed the government's Ministry of Information Technology to ensure that no such text was sent again ([Hindu Bureau, 2024](#)).

That the message came from a WhatsApp Business account also appeared to be in breach of WhatsApp's own guidance about how the platform should be used. The WhatsApp and Elections page explicitly states that 'Currently, political candidates and political campaigns are not permitted to

use the WhatsApp Business Platform’ ([WhatsApp, 2024c](#)). Meanwhile, the WhatsApp Business Messaging Policy available on the WhatsApp Business website explicitly prohibits political parties from using the WhatsApp Business Platform when it offers guidance on government and political use of the WhatsApp Business Platform as follows:

We permit the use of the WhatsApp Business Platform for government entities and require access through a Solution Provider (formerly known as Business Service Provider).

We prohibit the use of the WhatsApp Business Platform by Political Parties, Politicians, Political Candidates, and Political Campaigns.

We prohibit the use of the WhatsApp Business Platform by Law Enforcement Agencies, Military Services, National Security and Intelligence Agencies.

We prohibit the use of the WhatsApp Business Platform by entities that offer services related to politics, political candidates, political campaign strategy, political campaigning services, private companies that provide voting solutions and systems for elections, and exclusive government service providers. ([WhatsApp, 2024c](#))

The rules to keep WhatsApp Business separate from politics are very clear. Was the creation of a WhatsApp Business Platform account in the name of ‘Viksit Bharat Sampark’ a means for Modi to formally inaugurate his election campaign without the message being attributed to his political party or government?

Modi’s mass message became a topic of national discussion. Many citizens who received the message thought of the message as spam and, possibly, a scam. Other citizens viewed it as a violation of their privacy by the state, with many questioning how Modi and his team had access to what appeared to be a national database of phone numbers. Some questioned whether the government had used the database for Aadhar, the national identity number which is linked to citizens’ phone numbers, Under the Aadhaar Act, 2016, the 2018 Supreme Court judgment and the new Digital Personal Data Protection Act, 2023: that database is not meant to be used for political campaigning. The message also raised concerns about privacy and what data the government had because it was received not just by Indian citizens residing in India, but also by those living abroad and even foreign nationals in Pakistan and UAE who did not even have Indian phone numbers ([D’Cruze, 2024](#)). An opposition member of parliament, Saket Gokhale, asked the government to tell the citizens what database it had used ([Sarasvati, 2024](#)). At the time of writing this book, the government had not responded to this question. The Election Commission of India took no action aside from warning the government to stop sending bulk messages.

The message provoked discussion in online forums such as Reddit. One commentor there indicated that their phone number was not even linked to Aadhar and yet they still received Modi's message. The online news portal, The Wire, conducted a discussion on what bulk political messaging like this means for privacy ([The Wire Wrap Episode 6: Electoral Bonds, Kejriwal's Arrest, BJP's MCC Violation, 2024](#)). Lawyer Apar Gupta said that he reported it as spam. He might have used the 'Report Business' option that WhatsApp Business gives its users. WhatsApp blocks business accounts when enough users report them as spam. But Gupta claims he received the same message for a second time, indicating that the Viksit Bharat Sampark account might be using multiple phone numbers. Users also had an option to block the account, as one can do with messages received from WhatsApp Business accounts. But, as journalist Seema Chishti pointed out in the same discussion, some citizens might fear that 'blocking' the account could be equated with criticism of the government. The government, she says, might be maintaining a database of such preferences, and she 'might have revealed herself to be a datapoint' there. This fear reflected the government's general unwillingness to tolerate dissent, as we discussed in [Chapter 4](#).

The public debate around data privacy centred more on the government than WhatsApp and disappeared relatively quickly, despite the efforts of opposition parties to hold the government to account. The main opposition party, the Indian National Congress, wrote to Meta asking how it allowed a violation of its own policy, but did not seem to have received a response ([Livemint, 2019](#)). Congress Kerala's X (formerly Twitter) account posted the contents of the letter in a X (Twitter) thread on 16 March 2024:

This morning, Indian Citizens with WhatsApp has been getting an automated message from a 'WhatsApp verified Business' named Viksit Bharat Sampark. The message talks about taking feedback from Citizens, but the attached PDF is nothing but political propaganda.

In the guise of feedback, the letter is nothing but claims that Prime Minister @narendramodi is making about his Govt as part of his campaign for the upcoming General Elections, misusing govt database.

This is a blatant misuse of WhatsApp for political propaganda. WhatsApp's stated policy prohibits the usage of WhatsApp for political campaigns. If that's the policy, how do you permit a political leader to do propaganda on your platform? Or do you have a separate policy for BJP? ([INCKerala, 2024](#))

In the letter to Meta and the posts on X framed from the letter, the Congress wrote that the Viksit Bharat account is a 'verified Business' account and tells Meta that the message and pdf sent by Prime Minister Modi was a 'blatant misuse of WhatsApp for political propaganda' ([INCKerala, 2024](#)). On the

same Twitter thread, they posted a screenshot of the WhatsApp Business Policy section which prohibits governments and political parties from using the WhatsApp Business Platform. We could not find any report of Meta taking action against the Viksit Bharat Sampark account. The national government's public use of citizens' phone numbers, seemingly without consent, in combination with the possible bending of WhatsApp Business rules, presents a striking erosion of citizens' data privacy and a disregard for regulations designed to protect democratic practice.

Government of India and monetizing WhatsApp

Modi's use of a paid WhatsApp platform, apparently to bolster his political support, ironically follows a period when Indian financial and legal institutions had been reluctant to approve WhatsApp's new monetization infrastructure in the first place. The Indian government initially limited WhatsApp's access to its national payments interface. India was one of the markets where Meta conducted beta testing for WhatsApp Business and WhatsApp Pay, taking advantage of India's existing user base (De, 2024). WhatsApp also had to show patience for its payment gateway, WhatsApp Pay, to fully take off in India due to governmental regulations. WhatsApp Pay is built on the rails of India's Unified Payment Interface (UPI), which allows users to transfer money from their bank account via digital wallets to their contacts and make payments to businesses. Launched in 2016, the aim of UPI was to create a 'less cash' society by facilitating inter-bank transactions on a mobile platform. While WhatsApp Pay launched in India in 2020, the National Payments Corporation of India (NPCI) required a rollout in phases, with only 4 million users allowed in the first phase, 100 million allowed in the second phase by 2022, and the limit finally lifted on 31 December 2024 (Finextra, 2025). WhatsApp allows users to pay from the 'payment' section of their app through their UPI, which is connected to their bank account already. WhatsApp Pay entered a market where other payment apps such as Google Pay, Paytm, BHIM and PhonePe were already establishing themselves, but the ease of paying through an app which people already use for messaging was thought to be an advantage, and therefore also a potential threat to Indian founded or owned payments apps (Murphy and Findlay, 2020).

The Indian government also raised concerns about citizens' data privacy and security given that use of WhatsApp's payments gateway entailed Meta collecting data on Indian citizens' economic behaviour. The WhatsApp Payments Privacy Policy details how user metadata and data about transactions is shared with Facebook companies as well as with third-party service providers (WhatsApp, 2025h). The Indian government earlier sought clarifications from WhatsApp on how and where sensitive user data might be

stored by WhatsApp and WhatsApp had responded by stating that UPI pin and debit card details are not stored at all (Financial Express, 2018). However, the sharing of data across Meta companies remains a cause of concern. The Indian government also asked for data localization – that Indian data should remain in India – and for a WhatsApp office to be located in India before WhatsApp Pay could be rolled out (Agarwal, 2018).

Data localization had earlier become a point of conflict between Mark Zuckerberg and Mukesh Ambani, India's wealthiest businessman and owner of Reliance Industries, who is also seen as close to Narendra Modi. Ambani had criticized what he called Facebook's and Google's 'data colonialism' and pushed for data localization, arguing that India's data should be owned and controlled by India and not by American companies (Livemint, 2019). But since then, Ambani's tone has shifted. In 2020, Facebook bought a stake in one of Reliance's JioPlatforms and partnered with WhatsApp to build JioMart – India's first grocery delivery service where orders could be placed on WhatsApp. In 2023, Mark Zuckerberg and his wife, Priscilla Chan, attended the grand pre-wedding party of Ambani's youngest son in India, indicating the strength of the Ambani-Zuckerberg partnership (TechDesk, 2023). The successful monetization of WhatsApp through WhatsApp Business and WhatsApp Pay was also dependent on WhatsApp's 2021 privacy policy update which facilitated data sharing between WhatsApp and WhatsApp Business and subsequently third parties. As we detailed in Chapter 5, the Competition Commission of India and the Government of India both challenged WhatsApp in the courts, claiming the new terms of its privacy policy undermined an Indian citizen's right to privacy. A contradictory state-Big Tech relationship becomes further entrenched. On the one hand, party-political workers rely on WhatsApp's subterranean political infrastructure to campaign and organize while the party leader and Indian Prime Minister actively (mis)uses WhatsApp Business to mobilize political support. And on the other hand, the Indian government – through its legal and regulatory institutions – seeks to discipline and limit WhatsApp's power and authority. Against this backdrop WhatsApp actively promotes WhatsApp Business as something that is good for Indian society.

WhatsApp Business for social and economic good?

A part of the marketing strategy for WhatsApp Business is to present it as a benevolent product for businesses, especially SMEs in India. In 2018, the then WhatsApp Vice President Chris Daniels made a case to the Indian government that launching paid WhatsApp Business will help the country's economy grow (Singh, 2018b). At the time, WhatsApp announced funds for startups in India, joining hands with the government's body for promoting Startup India investments, Invest India (Outlook, 2018). As part of this

partnership, WhatsApp paid US \$250,000 as seed funding to the top five winners of the ‘WhatsApp Startup Challenge’, joined with the Confederation of the Indian Industry (CII) to train SMEs, and provided US \$250,000 to select entrepreneurs to promote their business number ([IndBiz, 2018](#)). This effort to financially support new businesses in India by partnering with government’s investment bodies in 2018 when WhatsApp Business was being tested was aimed at spreading awareness about WhatsApp’s new business tools. Ultimately, the assistance offered to Indian businesses helps WhatsApp’s business grow.

Today, the marketing of WhatsApp Business as a social good helps Meta deflect attention away from court cases that WhatsApp is embroiled in, as well as from the erosion of privacy caused through WhatsApp Business. In its presentation of itself as a benevolent actor working for the social good, Meta creates partnerships and offers skills training to small businesses in India. It also partners with government institutions. In 2023, WhatsApp India announced a partnership with the Open Network for Digital Commerce (ONDC) in India to work towards providing digital skills through the Meta Small Business Academy for up to 10 million entrepreneurs. Meta claims to provide a service not just to businesses but to India’s digital and economic growth by working towards greater ‘digital inclusion’. Sandhya Devanathan, Meta’s India Vice President said at the announcement of this partnership:

India’s digital transformation story is unfolding at a revolutionary pace, and for this *growth* to continue, we need the right ecosystem and partnerships that enable millions of small businesses to build and deepen their digital presence. Meta has been a frontrunner in partnering with the government and the industry to advance digital inclusion, especially for MSMEs across India. Our partnership with ONDC builds on supporting the government’s vision for Digital Public Infrastructure (DPI) and furthering our ongoing commitment to skilling small businesses and aiding this rapid digital transformation and growth story in the country. ([Meta, 2023b](#), emphasis added)

Presenting itself as a company that aids India’s digital transformation in line with the government’s Digital India initiative, Meta attempts to be on the government’s good side. Despite other areas of friction between the Indian government and WhatsApp, Meta’s portrayed synergies with the Indian government on the common goal of expanding the digital infrastructure for businesses.

In 2024, Meta hosted a WhatsApp India Business Summit where Devanathan again announced that WhatsApp was at the centre of India’s transformation ([WhatsApp, 2024b](#)). During her keynote speech, she spoke about how companies in India were using WhatsApp Business, WhatsApp

Payments and how even metro (underground railway) services in India's cities used WhatsApp Business for ticketing. She emphasized that for small businesses, WhatsApp was their 'website, digital storefront, and their livelihood'. She announced that they needed to be provided with more skills to use the WhatsApp Business app to its 'maximum potential'. She announced the 'WhatsApp Bharat Yatra' (WhatsApp India Journey) where WhatsApp employees travel across the country to give in-person training to small business owners to help them 'set up WhatsApp Business accounts, create "catalogs" and educate them on how to use click-to-WhatsApp ads' (WhatsApp, 2024b). Such a rhetoric of support is necessary for WhatsApp to show that it is not just profits that they are after but changing how people and businesses communicate. Arun Srinivas, director and head of Ads Business, Meta, India, in his speech at the summit, declared that people like to communicate with businesses through WhatsApp rather than having to make phone calls. He added that for many companies, WhatsApp communication leads to a growth in their sales and is the most effective medium for them to communicate.

Amid the narratives of innovation, effectiveness and growth, there was no talk of privacy. Descriptions of the summit on Meta web pages do not mention privacy at all. Is the promise that WhatsApp Business will transform India's economy a smokescreen or justification for the erosion of citizens' data privacy? Meta's framing of WhatsApp Business as not only an app to help businesses grow but to also enhance governance (such as ticketing for public transport) and aid India's economic growth has a subtext that is not explicitly stated – that Indians know what is good for them, and Meta is helping them, even if privacy is compromised. In this context WhatsApp Business was portrayed as an inevitable force for good that should not be stopped. But privacy is obscured in the WhatsApp Business narrative even as privacy remains key to the branding of WhatsApp.

WhatsApp and small businesses: professionalization, eroding trust and privacy?

Meta developed WhatsApp Business after observing how people in India (but also in Brazil and other countries) were creatively using the WhatsApp messaging app for their businesses. Recognizing the potential to monetize these organic practices, Meta used India as one of its primary testing environments before introducing the same products in what it sees as 'mainstream markets' (De, 2024). As we have shown, Meta sees India as a 'petri dish' for innovating WhatsApp for its global markets and growing the company's revenue (Cornish, 2023). This echoes a long history of the West using the non-West as a laboratory for developing scientific ideas that ultimately benefit the West (Tilley, 2001). WhatsApp for Business enables

Meta to monetize advertisements and announcements for businesses on a separate business app. WhatsApp Business' marketing as an innovative and professional app overshadows how the app also collects far more data about its users such as contact details, shopping activity, interactions with the Meta platforms and other third-party processes, such as AI chatbots to manage customer services. While users can limit some data sharing by using WhatsApp's privacy features, engagement with WhatsApp business inevitably gives Meta and other companies more insight into India's data economy and by extension, more power within the economy.

Since Indians were already doing business through the ordinary app, the question arises; to what extent does a specialized business app, with reduced privacy features, help them? For example, Sumedha Basu, who lives in Chhattisgarh in central India, has been using the ordinary WhatsApp app for her small saree business. Saree is an Indian garment for women where a 6-metre fabric is draped over a blouse and skirt. Sumedha buys sarees from the weavers and manufacturers and posts pictures on a WhatsApp group she created for her customers. The WhatsApp group has members from all over India who choose a saree from the pictures on the WhatsApp group and place an order with Sumedha. She started a WhatsApp group with a few of her friends and then their friends asked to be added:

My friends, who are interested in this, saw my friend wearing this [a saree] and liked it. They asked my friend where she had bought her saree. She told them about the WhatsApp group for selling sarees that I run. They asked to be added to my group.

Sumedha's contacts who were interested in buying sarees from her were happy to have this connection through WhatsApp, where they could buy sarees sitting at home. Similarly, some degree of acceptability of receiving customer service messages from WhatsApp Business accounts thus comes from WhatsApp already being a part of their everyday lives in multiple ways. Entrepreneurs creatively used WhatsApp to support their businesses even before Meta launched the special business app. They organically used features such as WhatsApp statuses, WhatsApp groups and broadcast lists to sell their products to those who were already on their contact list and then spread out to new contacts gained from existing networks.

Before the introduction of WhatsApp Business as a separate app, many in India already used WhatsApp to support their small businesses and continue to do so on their ordinary WhatsApp Business app. Indian businesses have always brought together their cultural and personal networks with professional ones (Graham and Marvin, 2001 in De, 2024) and WhatsApp users in India have been used to entrepreneurs reaching out to them through

personal networks. For entrepreneurs, users' willingness to buy on WhatsApp through networks they trust is what drove them to using WhatsApp in the first place. Local grocery shops, home cooks and bakers and do-it-yourself craft makers are some small businesses that started to use WhatsApp early on, combining their personal and business interests. WhatsApp Business in India is thus located at an already existing 'interplay of technological, social, and cultural dimensions' of Meta in India more generally (De, 2024). Hence, the coalescing of personal and professional networks on a private digital space like WhatsApp does not always seem jarring to all users, even as others might perceive it as a loss of privacy. In fact, WhatsApp adds a personal touch between sellers and potential customers and creates an element of trust that is often absent when people shop on a website (Talabi, 2022, p 73).

WhatsApp Business thus lands in India in a way that it commands trust, owing to its intimate medium of communication. In addition to trust, it is the most convenient form of communication as many people already use it. One of our respondents, Rohit Kumar, a photographer based in Goa, who uses WhatsApp Business, remarked,

The convenience, the convenience! See many apps have come even after that. People have tried emulating WhatsApp, but WhatsApp has become like Colgate. Nobody says toothpaste anymore, just send me a WhatsApp. Just send me, I mean, just pass me the Colgate, nobody asks you, can you pass me the toothbrush or the toothpaste.

Rohit's words indicate the ubiquity of WhatsApp in people's lives where 'WhatsApping' is the equivalent of digital messaging itself. Despite the techno-optimistic narratives espoused at the WhatsApp Business India summit 2024 and those that underpin Meta's drive to embed WhatsApp Business in India to improve customer experience, growth and efficiencies, not all businesses made the shift from WhatsApp to WhatsApp Business. We interviewed ten small business owners to get a sense of how they perceive WhatsApp for their businesses. All of them either used the ordinary WhatsApp app or the free WhatsApp Business app. If they used WhatsApp Business, they had both apps on their phones, to keep their business and personal conversations separate. But if they only used the ordinary WhatsApp app, they had their business and personal conversations on the same app. Since they relied on personal networks for their businesses, the ordinary WhatsApp app worked as a handy tool.

A home baker in Karnataka in south India, Ranjini Iyer, sells her baked goods through an ordinary WhatsApp account. She started her business during the COVID-19 lockdowns, relying on WhatsApp to sell her products to people around her, starting with family friends and neighbours. Her business took off only once her friends in the neighbourhood added her to

two existing WhatsApp groups, one meant for females in the neighbourhood and another where new businesses could pitch their ideas and products. She said that the connections between women entrepreneurs that WhatsApp enabled are what helped her start her business, and since the business is built on personal connections, she finds no need to use a WhatsApp Business account. We also met those who started out running a business using ordinary WhatsApp and then moved to a business account. Shefali Patekar, a business coach based in Maharashtra in western India, made the switch so that she could display her 'products' on the 'catalog' and present a more professional look. She told us:

because I was not able to put my products on normal WhatsApp. I was not able to put my work hours. I wanted a little professional look. If you are a coach, working with business owners, you have to maintain that level of professionalism ... And when we go out and talk, in social networking, in events, people say that you are running a business with traditional WhatsApp. So, that gives a little feel. And when a new person connects with me, they know about my products, they know about the product before the discussion. So it becomes easier for me to explain to him. I don't have to talk to him I don't have to say anything. He would go and just have a look at my profile. He would check the product. People would ping me directly from there and message me on WhatsApp that you have to subscribe to this product. It becomes easier for me.

When asked what is it about WhatsApp that makes it 'easier', she told us: 'It's become a habit. It's easy to understand. It's very friendly. The culture of WhatsApp is easy to understand. The interface is easy. I would say that no one needs to write. Someone can send audio as well. It works fast.' The words 'easy', 'fast' and 'friendly' point to how WhatsApp's user-friendliness makes it the preferred messaging app for everyone in India. That WhatsApp can provide tools to 'professionalise' one's profile brings an added advantage. The accessibility of WhatsApp for potential clients drives entrepreneurs to using WhatsApp as a personal-professional tool. It also shows how Ranjini is on board with Meta's vision of the separate business app being more professional and efficient.

Sumedha Basu, our respondent who runs a saree business through WhatsApp, uses both the ordinary WhatsApp app and WhatsApp Business to support her two businesses on the same smartphone. Her second business, where she worked as an independent business consultant, is what she used WhatsApp Business for. It was common for users like her to use both apps to run their businesses. Ranjini also figured that she got more orders for her cakes through WhatsApp than Instagram.

Rohit, a photographer based in Goa, liked doing business through WhatsApp Business as it helped him talk and negotiate with clients on a ‘personal level’ while looking ‘professional’, just as Shefali pointed out too. He also felt that clients who communicated with him through WhatsApp tended to ‘reconnect’ more if they liked his work. Hetal Shah, who runs a custom-made stationery business in Gujarat, western India, found WhatsApp to be safe since she knew most of the people she communicated with through the app, so she trusted the customers to pay the money and not steal her designs: ‘70 per cent of the people who know us, are from the same place ... So it (WhatsApp) is safer than other platforms’. The user-friendliness of WhatsApp and WhatsApp Business, alongside the intimacy, the feeling of relative safety and the possibility of directly reaching potential customers helps small and independent businesses to rely on it to set up or expand their customer base. As small business owners struggle with the resources and technology to set up websites, WhatsApp presents an effective and readily available medium (Narayan and Narayanan, 2024, pp 229–230).

The use of WhatsApp by women entrepreneurs also indicates how WhatsApp supports home-based businesses which do not require capital to set up premises. Businesses such as Ranjini’s home-baking and Sumedha’s saree business functioned through personal connections and did not necessarily require the WhatsApp Business app. Sumedha used WhatsApp Business for her second business which required a more ‘professional’ interface. Women are more likely to use messaging apps for business whereas men engage in more traditional jobs or traditional forms of running businesses (De, 2025). The intimacy of WhatsApp helps women connect with each other, without always needing to create a professional catalogue on WhatsApp Business.

But women and men alike do draw on specific features of the Business app that they find convenient for their business. Rohit Kumar, for example, was an avid user of many features of WhatsApp Business. He liked to use the ‘Away’ message feature when he is on photo shoots. He told us: ‘So whenever the client messages me and I’m unable to take it, automatically an auto message goes to them. Thank you for contacting so and so person and in case I’m not available, please contact so and so number.’ In offering such features, WhatsApp Business works as a replacement for email. It is not as intimate as the ordinary WhatsApp app but clients can easily be informed through the app’s affordance if the business owner is away. Hetal finds using the catalog feature very helpful as customers can place orders for products by seeing the photos of the samples. Vijay Dhakad, who runs a spice business, also finds the catalog feature to be very useful, alongside the more general features of WhatsApp such as being able to send videos and voice notes to customers who are located in rural areas.

However, despite its advantages, WhatsApp Business is also frustrating for some users. Drishil, who runs a hardware store in Bangalore in south India, said very strongly: 'WhatsApp Business is so much a waste. WhatsApp Business is absolutely a waste. It makes no difference to me.' When asked why, he responded,

There is nothing in it. See, I am one of the earliest users of WhatsApp Business in India. I think I am one of the first 1 million users of WhatsApp in India. That's how early I got it. But it makes no difference. See, it is such a big pain. On WhatsApp Business, you can add your products and services' photo. Like an online catalog and such if you know. So it's an absolute pain to add things in that. I can't add stuff to my browser I'm not able to add stuff through my cell phone. So I stopped using it whatsoever. It's not easy to click, drag, crop, add, add groups, add photos it's not as easy as it looks so I stopped using WhatsApp Business at all.

Drishil clearly found WhatsApp Business tedious. Others found roadblocks. Arun Kannan who runs a fresh fish supply business by taking orders on WhatsApp, could not post pictures of the fresh catch of fish on the WhatsApp Business catalog:

Because we are selling fish and kind of which comes under animal category, some protocol no? We can't sell cigarette; we can't sell something like that online like that. Some protocol on animal products ... I don't know how to message or like who to contact for WhatsApp for this kind of issue ... This is like a consumable item. So it comes under that protocol. I wasn't able to create a catalog.

Not being able to contact anyone at WhatsApp about this issue meant that Arun had to work around the problem himself. When his photo upload verification on the catalog was rejected, he simply sent the fish photos on WhatsApp groups, direct to existing customers. Having the WhatsApp Business app did not give him an added advantage in this case as he would have sent photos on the ordinary WhatsApp app. What is notable is that people always work around technology and domesticate it to fulfil their needs.

The professionalizing zeal behind Meta's push for WhatsApp Business did not always work to the benefit of all entrepreneurs. According to [De \(2025\)](#), the formalized and so-called professional interface of WhatsApp Business alters the dimensions of care, wellbeing and protection that came to define doing business on WhatsApp in the first place. By taking away the informality of business on WhatsApp, Meta seeks to create more impersonal,

corporatized spaces of WhatsApp Business. That takes away the informality, trust and personal touch which were the reasons why WhatsApp became a place for intimate business. The ‘digital colonialism’ of WhatsApp Business is evident in how a Big Tech company reinforces the imbalance of power by disrupting informal creative practices when it introduces standardization (De, 2025, drawing on Couldry and Meijas, 2019; Mohamed et. al, 2020; Adamu 2023). Her respondents struggled to adapt to Meta’s ‘coercive professionalisation’ which required figuring out a different app altogether. Many decided to stick to doing business through the ordinary app rather than moving to the business app. In presenting itself as the saviour of businesses in the global south, Meta follows the script of digital colonization where informality as well as privacy are sidelined.

WhatsApp Business is now widely used by businesses in India, who make it work for them through and despite the app’s features and controls. There may be success stories, as WhatsApp’s websites highlight, but there are also frustrations with WhatsApp Business and a lack of interest in doing one’s business communications through it. In trying to professionalize and monetize WhatsApp, Meta also makes users share more data and unwittingly accept lower privacy protections on the app. Our respondents who used WhatsApp Business largely did not think about the privacy settings they might have agreed to in using it. The erosion of privacy here took place due to the discursive sidelining of it.

Conclusion

The transformation of WhatsApp into a key tool for business has relied on and contributes to the erosion of users’ data and everyday privacy in different ways. This chapter has shown how WhatsApp Business presented Meta with the opportunity to monetize its users’ attention in a way that WhatsApp’s digital private messaging service alone could not. The development and implementation of WhatsApp business by Meta not only exploits its users’ networked private lives, attention and trust, but also profits from the practices of entrepreneurs in India and other key markets in the global south, who were organically innovating and experimenting with the WhatsApp app for their businesses.

The potential for WhatsApp Business depended on shifting data relations whereby WhatsApp weakened users’ data protections to transfer power and profit to Meta. The receipt of spam and scam messages sent through WhatsApp Business Platform accounts has tangibly altered the intimate and personal nature of WhatsApp’s digital private spaces; meanwhile users’ informational privacy is undermined by the belief that one’s phone number is public property and essential for their participation in economic life. By pitching WhatsApp Business as a social and economic good, Meta constructs

its new product as an invaluable and inevitable digital solution for driving India's economic growth. This techno-optimistic narrative emphasizes India's economic future while simultaneously obscuring two key issues: the erosion of user's privacy required to expand Meta's data extractive practices and the extent to which Meta's own economic future is central to this business model. WhatsApp is now in business.

Conclusion

We began this book with the fracture between Sabeena's uncertain and arduous experience of maintaining not just her own, but also her friends' privacy on their WhatsApp chats in New Delhi. Their privacy work was informed by the legacies of (global) corporate and post-colonial state surveillance, violence and mistrust. And on the other hand, Meta CEO Mark Zuckerberg's optimistic declaration to a conference hall in San Jose a year earlier that the 'future is private' for 'social platforms'. His vision was underpinned by a shift in the company's technical architecture and promoted WhatsApp as the archetypal model of privacy values and technical best practice, embodied in its end-to-end encrypted messaging by default.

The relationship between the techno-imaginary of WhatsApp as a digital private space and how a private digital technology *actually* 'lands' and is informed by and through different topographies was the focus of the book. We questioned; who was this private future imagined for, and why? And what does privacy and the private look and feel like in practice? Recognizing from the outset that privacy is suffused with uneven power relations, we contend that in the context of global digital technologies, privacy is not only political but also geopolitical.

Privacy is also sociotechnical and transformed through the shifting relationships between Big Tech, states, civil society and citizens. The argument we make throughout the book is that WhatsApp and Meta have productively engaged and struggled over privacy – as a discourse and legal right, and by design and experience – to further its corporate power and profit. This appears somewhat paradoxical. Informational capitalism is built upon the collection, processing and commercialization of data which thrives in conditions of less, not more privacy.

In a globally networked world where digital privacy – as idea, practice and thing – is context dependent, then conceptualizing privacy on a planetary scale is essential. Through a feminist geopolitics of privacy, *Privacy Techtonics* makes privacy the subject, to understand not what privacy is, as an end goal or output, but how privacy is struggled over in situ. In this case, how digital

private messaging and digital privacy with respect to WhatsApp is narrated, negotiated and contested within India's national politics, the law, design and everyday experience.

Privacy studies have typically deliberated over privacy definitions or focused on apparently independent privacy matters concerning, for example, privacy policies and law, incidents of privacy harms or embedding privacy-by-design. With the focus on WhatsApp this book has advanced a more encompassing, multiscalar and multi-sited framework. Read together, these highlight the connections between different dimensions of privacy and the different sites and scales through which WhatsApp is designed and domesticated.

Privacy Tectonics therefore opens up space to witness a diversity of privacy stories and their constitutive people, things and relationships. With our focus on India as WhatsApp's largest market by far, the so-called 'digital peripheries' of the global south are central to WhatsApp's future ambitions and to the book's argument. Seeing WhatsApp from India and the everyday disrupts the western and patriarchal idea of a digital private future as a universal 'good'. Our research surfaces the complex and contradictory ways in which privacy is unevenly productive of power within the context of India's post-colonial state, corporate authority and an emergent national data and privacy protection landscape.

WhatsApp is built on the privatization of the internet, parcelled up into digital enclosures which are just as likely to undermine democratic practices as they are to promote them. In India, digital enclosures have concentrated power in the private authority of WhatsApp/Meta which derives value from the collection and processing of data points concerning how we engage in and between digital private spaces. Meanwhile the Hindu right have powerfully harnessed WhatsApp's subterranean storytelling infrastructure and human capacity for sharing to deepen its Hindu nationalist project through targeted and discriminatory messaging beneath the radar of public scrutiny.

Meta and WhatsApp's privacy discourses position privacy and private futures as an inevitable marker of progress in our 'digital lives'. The public pivot to privacy served as a tonic to refresh and revitalize Facebook's reputation, damaged by the publicity surrounding its public data-sharing practices. This reinforces the importance of privacy for building and maintaining user trust, where trust is crucial corporate currency. Privacy is competitive. Competition between Big Tech corporations plays out not just around technology and turnover but crucially over the extent to which their imaginaries captivate the public (Natale et al 2021). It is hard to question or challenge a company that centres privacy in their mission. Yet as Ari Waldman (2021) shows, corporate privacy agendas are often anti-privacy in practice. The un-making of WhatsApp's privacy policy was masked by the addition of new 'privacy layers' which individualized user control and responsibility.

Privacy visions are routed through privacy things. Building on Santos and Faure (2018) we illustrate how end-to-end encryption represents a form of code power that is strategically mobilized within global intimate spheres. End-to-end encryption as security infrastructure is used in the service of elevating WhatsApp's reputation as the global protector of privacy. Following the public backlash to WhatsApp's privacy policy updates, end-to-end encryption was used to redirect public and legal attention. By publicizing the significance of encryption for protecting the content of personal messages to users, the relevance of the metadata attached to that message, the user and their network remains obscured and protected for WhatsApp to reproduce its 'coloniality of power' through data (Ricaurte, 2019).

Privacy things and the metaphors and media campaigns that make them knowable and visible are political. WhatsApp/Meta's analogy of the 'digital living room' relies on patriarchal and western constructs of the domestic as a site of security and sanctuary for all. Yet, citizen-user privacy experiences illustrate how the domestic and the geopolitical are intertwined and the promise and feeling of privacy is unevenly realized. While most people engage in degrees of (digital) privacy work, the burden of work falls to minoritized individuals for whom the risk of data leaks, hacks and surveillance are highest. WhatsApp's new 'privacy layers' afford users additional features that imitate the informal workarounds they already employed. Though these make privacy work less arduous they reinforce the notion that privacy is an individual's responsibility. Again, these privacy things deflect attention from the fact that data collected from attention on the app alone provides everything WhatsApp needs to commodify digital private lives.

In India, the addition of WhatsApp's new 'interlocking layers of protection' coincided with the roll out of WhatsApp Business, its success dependent on the suck of WhatsApp's network effect and the erosion of WhatsApp's data principles and privacy. With WhatsApp now in business, the significance of privacy has been overtly and subtly relegated. This personal and national trade-off is justified through narratives that frame WhatsApp Business as indispensable both to small and medium business owners and for India's future socio-economic growth. Narendra Modi's office meanwhile hacks WhatsApp's terms of service and capitalizes on the ubiquity of data to send unsolicited messages to the nation's WhatsApp accounts.

In a more recent development, WhatsApp is positioning itself as 'India's gateway to the world of AI' and capturing the imagination of business and government startups who are building AI assistants on top of Meta's Business API to engage directly with customer/citizens and avoid the friction of 'downloads, logins and learning curves' (Shaikh, 2025). Most Indians in rural areas use AI only through WhatsApp. Given the rapid early AI adoption, Sandhya Devanathan, Head and VP of Meta in India describes how India is yet again a 'testbed', only this time the focus is on 'how a billion people

access AI and shape habits'. With business and government valuing the scale and ubiquity of WhatsApp for interfacing with customers and citizens alike, their engagement is accelerating and entrenching India's dependency on Meta, a private company. As AI now lies at the heart of Mark Zuckerberg's imagined future and ambitions to further corporate power, future research on the intimate geopolitics of AI and privacy is vital.

We close by reflecting on how, until recently, WhatsApp was relatively unknown in the US where most of its population are historically Apple iPhone and iMessenger users by default. But as Meta's 2024 Earnings calls revealed, the US is now WhatsApp's fastest growing market, recently hitting a 100 million monthly active users. This is something Zuckerberg is extremely excited about, as he recognized that their efforts to grow WhatsApp and mature the business in the rest of the world could now result in 'a big tailwind if the US ends up being a big market'. As Zuckerberg implied, having tested WhatsApp in the 'petri dish' over 'there' it could now reap dividends 'here' in the US, even with a small national share of the messaging market 'because the United States punches above its weight in terms of, it's such a large percent of our [Meta's] revenue' (Platforms, 2024). This sentiment echoed that of Will Cathcart, WhatsApp's CEO, speaking a year earlier to the *New York Times* about his company's goal: 'to make WhatsApp a household name [in the US], whether it is to shop, chat or stay on top of news and events'. He explained that now 'The conversation has moved from "WhatsApp is the app I use outside the US when I travel" ... It's becoming significantly more mainstream' (Issac, 2023). While it might be 'pretty fun' for Zuckerberg to see people around him in San Francisco using WhatsApp, his and Cathcart's unvarnished opinions connote the Silicon Valley worldview that regards the US as 'mainstream' and privacy as a useful discursive, legal and technical tool to help mature WhatsApp's business, all in the pursuit of profit.

APPENDIX

Methodology

Research for this book was conducted between 2019 and 2024 and involved five phases. In carrying out research we, the co-authors Philippa Williams and Lipika Kamra, were supported by the excellent work of six researchers who were employed at different times on the project: in alphabetical order, Zaheeb Ajmal, Shruti Arora, Pushpendra Johar, Fatma Matin Khan, Mukesh Kumar and Ekta Oza. We are indebted to their work and have published earlier iterations of our research together; see [Williams et al \(2022\)](#), [Kamra, Williams and Johar \(2023\)](#), [Arora \(2023\)](#) and [Oza, Williams and Kamra \(2024\)](#).

The first phase of research was conducted in the northern Indian cities of New Delhi and Varanasi, Uttar Pradesh between February and June 2019, during and after the Indian national elections 2019 and by a team of four field researchers, two based in each city. Fatma Matin Khan and Ekta Oza researched in New Delhi, and Pushpendra Johar and Mukesh Kumar in Varanasi. Following a residential workshop in Delhi, we implemented an ethnographic approach that privileged locating and interpreting individual narratives, experiences and practices of using digital technology within everyday contexts ([Horst and Miller, 2012](#); [Pink et al, 2016](#)). This drew on principles of participant observation, everyday conversations and 70 in-depth interviews with ordinary citizens and 20 interviews with party-political workers and volunteers across the two cities. Our ethnographic approach focused on locating and interpreting individual narratives, experiences and practices of using digital technology and consuming ‘extreme speech’ within everyday contexts and social political histories ([Horst and Miller, 2012](#); [Pink et al, 2016](#); [Banaji and Bhat, 2022](#)). Researchers also collected WhatsApp messages, memes and videos that respondents shared with us.

The second phase of research was carried out in 2020 during the COVID-19 crisis in New Delhi and Patna, a city in the northeastern state of Bihar. Recognizing the significance of WhatsApp during COVID-19, Pushpendra, a New Delhi resident and a member of the original research team, was hired to carry out further research between March and May 2020. During

this period, Pushpendra, like other Delhi residents, was subject to both national lockdown and subsequently containment zone rules so we adapted our research strategies and shifted to primarily online spaces. This period of research involved: (1) participant observation by Pushp and Lipika on Delhi neighbourhood WhatsApp groups which offered an insight into how groups were being mobilized during lockdowns for surveillance as well as care; (2) Philippa and Lipika closely followed Indian news outlets and social media; and (3) Pushpendra conducted online interviews with 16 people to understand how the pandemic had impacted digital urban lives. The interviews were conducted on Skype, Zoom and by phone to suit the participants' preferences. Pushpendra accessed research participants through existing networks and subsequent snowballing. Interestingly, Pushpendra found that online interviews naturally lasted much longer compared to those he conducted for the project pre-pandemic, as participants who were quarantined at home had more time and were eager to share their digital urban experiences of the pandemic. In Patna, Zaheeb Ajmal conducted research in the run up to the Bihar state assembly elections. While we had not conducted research in Bihar in Phase 1, we decided to conduct research there as this was the first election in India to be held during COVID-19 and politicians had to rely much more on digital campaigning than ever before. Between September and November 2020, Zaheeb interviewed ten people (online and offline), which included political party actors and voters. He also collected the messages, memes, and videos circulating on WhatsApp during the campaign phase of this election.

The third phase involved a shift in the focus of our research. In 2021, after WhatsApp announced a controversial privacy update, we decided to bring in a focus on sociodigital practices of privacy in everyday life, and especially vis-à-vis WhatsApp. Shruti Arora conducted 34 interviews with citizens in New Delhi between June and August 2022. Additionally, Shruti, Philippa, and Lipika interviewed 11 experts: privacy and civil society activists, legal scholars, lawyers and technology journalists. The focus of these interviews was on privacy rights activism, privacy-by-design and India's regulatory landscape around digital privacy.

The fourth phase of research centred on the growing use of WhatsApp for Business messaging in India and its implications for perceptions and experiences of privacy. From September to December 2023, Pushp interviewed a further 20 people. Ten of these were business owners who either used the ordinary WhatsApp app or used the WhatsApp Business app. The other ten interviewees were customers who ranged from those who communicated with businesses on WhatsApp to those who hated receiving messages from businesses. These interviews were conducted online with participants located across India, in New Delhi, Gurugram, Ghaziabad, Allahabad, Bilaspur, Pune, Goa, Kochi, Hyderabad, Bengaluru and Chennai.

The four phases of field research contributed to the empirical material found in this book. We have used pseudonyms for research participants' names, as well as for the WhatsApp groups and localities in which they reside to protect the identities and relationships of those involved in the research. The names of civil society activists and journalists are not anonymized. We were careful not to use material from WhatsApp groups where we did not have permissions from all participants. The interviews in all phases were conducted in Hindi, English or both. The interviews were transcribed and translated by the researchers, and original phrases were retained to convey culturally specific meaning (Jazeel, 2016). While our interviewees intersected different generational, gender, caste and religious identities, the majority of research participants either owned or had access to a smartphone on which they used WhatsApp and were generally middle or upper class. This is in part a reflection of the digital divide that persists as well as access afforded by our researchers. Consequently, scope remains to study the use of WhatsApp among working classes, within more rural areas and with a more explicit focus on caste as an intersectional experience and also among speakers of other Indian languages.

During Phase 5, from 2021 to 2024, Philippa and Lipika carried out discourse analysis of Meta financial (Q-10) reports and earnings transcripts, WhatsApp and Facebook/Meta terms of service, privacy policies and blogs. We analysed media interviews with Facebook and WhatsApp executives as well as the companies media campaigns and advertisements in India and the UK. We are grateful for the existence of and access to the 'The Zuckerberg Files' created by Michael Zimmer as a digital archive of all publicly available statements and appearances of CEO Mark Zuckerberg (available here: <https://zuckerbergfiles.org/>), 'The Facebook Papers' which report on the documents provided by Francis Haugen to Congress and global news outlets (available here: <https://facebookpapers.com/>) and the Wayback machine at the Internet archive from where we accessed WhatsApp's historical webpages <https://web.archive.org/>.

We also analysed the archive of legal documents pertaining to WhatsApp's litigation in India, for example affidavits, petitions, suo moto proceedings, case reports, for example, *Competition Commission of India, Chaitanya Rohila v Government of India, Facebook v CCI, WhatsApp v CCI, Karmanya Singh Sareen v Union of India*, and read in the context of the Indian Constitution, Indian government policy, web content and press releases as well as civil society reports by among others, Internet Freedom Foundation.

The first two phases of the project were funded by a WhatsApp Misinformation and Social Science Research award. For us, the funding of academic research by tech giants raised significant ethical and practical questions concerning our positionalities, the monetization of research, access to data and audience trust. We were, and remain, somewhat ambivalent

about how our relationship with Facebook has coopted us into the tech giant's agenda. But we are reassured to some degree that WhatsApp did not provide us with any user data, and we are free to publish our findings anywhere. From this vantage point, we see our role as contributing critically to debates on Big Tech without being pulled into Facebook's orbit. We are also cognizant of concerns about audience trust in the independence of our findings. As a human geographer and a political anthropologist, we are primarily concerned with privileging research participants' narratives and experiences in our analysis and are under no tacit or contractual obligations to portray WhatsApp in a particular way. Indeed, other recipients of the award have already published critical accounts of the messaging platform (see [Banaji and Bhat, 2019](#); [Hitchen et al, 2019](#)). We are mindful of the challenge of researching ethically in 'a digital world as degraded and depraved as it is delightful' and accepted the funding in the spirit of critical engagement while recognizing our complicity in the digital world (see [Markham, 2020](#), p 116). We have written in detail about the politics of Big Tech funding in [Williams et al \(2022\)](#). Phases 3 to 5 were funded by a Phillip Leverhulme Prize in Geography awarded to Philippa by the Leverhulme Trust.

Bibliography

- Adamu, M.S. (2023). No more “solutionism” or “saviourism” in futuring African HCI: A manifesto. *ACM Transactions on Computer-Human Interaction* 30(2), 1–42.
- Adorno, T. (2019). *The Authoritarian Personality*. Verso.
- Agrawal, A. (2021). Facebook, WhatsApp sue Indian government over traceability requirement. *Forbes India*. <https://www.forbesindia.com/article/take-one-big-story-of-the-day/facebook-whatsapp-sue-indian-government-over-traceability-requirement/68175/1>
- Agarwal, S. (2018). WhatsApp payments hit office hurdle. <https://economictimes.indiatimes.com/industry/banking/finance/banking/whatsapp-payments-hit-office-hurdle/articleshow/65221167.cms?from=mdr>
- Ali, M. (2020, 14 April). The rise of a Hindu vigilante in the age of WhatsApp and Modi. *Wired*. <https://www.wired.com/story/indias-frigntening-descent-social-media-terror/>
- Allen, A. L. (1988). *Uneasy Access: Privacy for Women in a Free Society*. Rowman & Littlefield.
- Amrute, S. and Murillo, L. F. R. (2020). Introduction: Computing in/from the South. *Catalyst: Feminism, Theory, Technoscience*, 6(1), 1–23.
- Anderson, E. and Longkumer, A. (2018). ‘Neo-Hindutva’: Evolving forms, spaces, and expressions of Hindu nationalism. *Contemporary South Asia*, 26(4), 371–377.
- Andrejevic, M. (2002). The work of being watched: Interactive media and the exploitation of self-disclosure. *Critical Studies in Media Communication*, 19(2), 230–248. <https://doi.org/10.1080/07393180216561>
- Andrejevic, M. (2009). Privacy, exploitation and the digital enclosure. *Amsterdam Law Forum*, 1(4), 47–61.
- ANI. (2021, 19 July). Pegasus Spyware: Reports of hacking ‘false, misleading’, says Israeli firm. *The Times of India*. <https://timesofindia.indiatimes.com/india/pegasus-spyware-reports-of-hacking-false-misleading-says-israeli-firm/articleshow/84547543.cms>
- Anonymous. (2018). An interview with Chris Daniels, CEO of WhatsApp. <https://www.fishsensedq.com/interview-chris-daniels-ceo-whatsapp/>

- AP. (2016, 2 March). Top Facebook executive released from Brazilian jail. *The Guardian*. <https://www.theguardian.com/technology/2016/mar/02/brazil-police-release-top-facebook-executive-from-jail>
- AP. (2020). India restores internet in Kashmir after 7 months of blackout. Al Jazeera. <https://www.aljazeera.com/news/2020/3/5/india-restores-internet-in-kashmir-after-7-months-of-blackout>
- Appadurai, A. (2006). *Fear of Small Numbers: An Essay on the Geography of Anger*. Duke University Press.
- Arora, P. (2016). The bottom of the data pyramid: Big Data and the global south. *International Journal of Communication*, 10, 1681–1699.
- Arora, P. (2019a). Decolonizing privacy studies. *Television & New Media*, 20(4), 366–378. <https://doi.org/10.1177/1527476418806092>
- Arora, P. (2019b). *The Next Billion Users: Digital Life Beyond the West*. Harvard University Press.
- Arora, P. (2019c). Politics of algorithms, Indian citizenship and the colonial legacy. In A. S. M. Punathambekar (Ed) *Global Digital Cultures: Perspectives from South Asia*. University of Michigan Press.
- Arora, P. and Scheiber, L. (2017). Slumdog romance: Facebook love and digital privacy at the margins. *Media, Culture & Society*, 39(3), 408–422. <https://doi.org/10.1177/0163443717691225>
- Arora, S. (2023). Researching and reflecting on experiences of digital privacy in India. *GenderIT.org*. <https://www.genderit.org/articles/researching-and-reflecting-experiences-digital-privacy-india>
- Arun, C. (2019). On WhatsApp, rumours, lynchings, and the Indian Government. *Economic & Political Weekly*, 54(6). <https://www.epw.in/journal/2019/6/insight/whatsapp-rumours-and-lynchings.html>
- Aryan, A. (2021, 20 May). Govt again warns WhatsApp to scrap the 2021 privacy policy. *The Indian Express*. <https://indianexpress.com/article/technology/social/whatsapp-should-withdraw-new-privacy-policy-says-meity-in-new-notice-7321535/>
- Asher-Schapiro, A. (2020, 24 February). After WhatsApp spyware allegations, Indian journalists demand government transparency. *Committee to Protect Journalists*. <https://cpj.org/2020/02/whatsapp-spyware-allegations-indian-journalists-government/>
- Ashlin, M. (2021, 13 January). WhatsApp ad in newspapers is deceptive, spreading misinformation, say tech policy experts. *Deccan Herald*. <https://www.nationalheraldindia.com/india/whatsapp-ad-in-newspapers-is-deceptive-spreading-misinformation-says-tech-policy-experts>
- ASPICanberra. (2021). ASPI webinar: In-conversation with Will Cathcart, Head of WhatsApp. YouTube. <https://www.youtube.com/watch?v=2KbQC5LDoBA>

- Atal, M. R. (2021). The Janus faces of Silicon Valley. *Review of International Political Economy*, 28(2), 336–350. <https://doi.org/10.1080/09692290.2020.1830830>
- Attwood, F., Hakim, J. and Winch, A. (2017). Mediated intimacies: Bodies, technologies and relationships. *Journal of Gender Studies*, 26(3), 249–253. <https://doi.org/10.1080/09589236.2017.1297888>
- Auxier, B., Rainie, L., Anderson, M., Perrin, A., Kumar, M. and Turner, E. (2019). Americans and privacy: Concerned, confused and feeling lack of control over their personal information. *Pew Research Center*. <https://www.pewresearch.org/internet/2019/11/15/americans-attitudes-and-experiences-with-privacy-policies-and-laws/>
- Balkin, J. M. (2017). Free speech in the algorithmic society: Big Data, private governance, and new school speech regulation. *Yale Law School, Public Law Research Paper*, 615. <https://doi.org/10.2139/ssrn.3038939>
- Banaji, S. and Bhat, R. (2019). WhatsApp vigilantes: An exploration of citizen reception and circulation of WhatsApp misinformation linked to mob violence in India. <https://www.lse.ac.uk/media-and-communications/assets/documents/research/projects/WhatsApp-Misinformation-Report.pdf>
- Banaji, S. and Bhat, R. (2022). *Social Media and Hate*. Routledge.
- Banerjee, M. (2014). *Why India Votes?* Routledge.
- Banerjee, M. (2021). *Cultivating Democracy: Politics and Citizenship in Agrarian India*. Oxford University Press.
- Banka, R. (2021). Don't use WhatsApp if concerned about data: Delhi HC. *Hindustan Times*. <https://www.hindustantimes.com/india-news/dont-use-whatsapp-if-concerned-about-data-delhi-hc-101610961072770.html>
- Bapna, A. (2023, 14 September). Inside Meta's monumental privacy campaign for WhatsApp in India. *The Drum*. <https://www.thedrum.com/news/2023/09/14/inside-metas-monumental-privacy-campaign-whatsapp-india>
- Barbosa, S. (2023). The rise of WhatsAppers from the global south [Interview]. <https://www.iwm.at/news/sergio-barbosa-the-rise-of-whatsappers-from-the-global-south>
- Barnett, C. and Low, M. (Eds) (2004). *Spaces of Democracy: Geographical Perspectives on Citizenship, Participation, and Representation*. Sage.
- Baulch, E., Matamoros-Fernández, A. and Johns, A. (2020). Introduction: Ten years of WhatsApp: The role of chat apps in the formation and mobilization of online publics. *First Monday*, 25(1–6 January 2020).
- Baxter, R. and Brickell, K. (2014). For home unmaking. *Home Cultures*, 11(2), 133–143.
- BBC. (2018, 15 January). Netanyahu and Modi praise 'new era' in India – Israel ties. *BBC News online*. <https://www.bbc.co.uk/news/world-asia-india-42686597>

- Bear, L. (2020). Speculation: A political economy of technologies of imagination. *Economy and Society*, 49(1), 1–15. <https://doi.org/10.1080/03085147.2020.1715604>
- Beckert, J. and Bronk, R. (Eds) (2019). *Uncertain Futures: Imaginaries, Narratives, and Calculation in the Economy*. Oxford University Press.
- Benjamin, R. (2019). *Race After Technology Abolitionist Tools for the New Jim Code*. Polity.
- Bhagchandani, D. (2024, 17 September). 15 surprisingly insightful WhatsApp statistics every marketer should know. <https://doubletick.io/blog/whatsapp-user/#:~:text=9.,WhatsApp%20Business%20Statistics,with%20approximately%20128.4%20million%20downloads.&text=%E2%80%8BDaily%2C%20around%20175%20million,reviews%2C%20as%20Sensor%20Tower%20reported>
- Bhan, G. (2016). *In the Public's Interest Evictions, Citizenship, and Inequality in Contemporary Delhi* University of Georgia Press. <http://www.jstor.org.ezproxy.library.qmul.ac.uk/stable/j.ctt19x3jp8>
- Bhat, R. (2020). *The Politics of Internet Infrastructure: Communication Policy, Governmentality and Subjectivation in Chhattisgarh, India*. Doctoral dissertation. London School of Economics and Political Science.
- Birhane, A. (2020). Algorithmic colonization of Africa. *SCRIPT-ed*, 17(2), 389–409.
- Blunt, A. and Varley, A. (2004). Geographies of home. *Cultural Geographies*, 11(1), 3–6.
- Boellstorff, T. (2016). For whom the ontology turns: Theorising the digital real. *Current Anthropology*, 57(4), 387–407.
- Bossetta, M. (2018). The digital architectures of social media: Comparing political campaigning on Facebook, Twitter, Instagram, and Snapchat in the 2016 US Election. *Journalism & Mass Communication Quarterly*, 95(2), 471–496. <https://doi.org/10.1177/1077699018763307>
- Boyd, D. and Marwick, A. E. (2011, 22 September). Social Privacy in Networked Publics: Teens' Attitudes, Practices, and Strategies. *A Decade in Internet Time: Symposium on the Dynamics of the Internet and Society*. <https://ssrn.com/abstract=1925128>
- Boyle, J. (2003). The second enclosure movement and the construction of the public domain. *Law and Contemporary Problems*, 66(33), 147–178.
- Bratton, B. H. (2015). *The Stack: On Software and Sovereignty*. MIT Press.
- Braverman, I., Blomley, N., Delaney, D. and Kedar, A. (Eds) (2014). *The Expanding Spaces of Law: A Timely Legal Geography*. Stanford University Press.
- Brickell, K. (2012). Geopolitics of home. *Geography Compass*, 6(10), 575–588. <https://doi.org/https://doi.org/10.1111/j.1749-8198.2012.00511.x>
- Brickell, K. and Cuomo, D. (2019). Feminist geolegality. *Progress in Human Geography*, 43(1), 104–122. <https://doi.org/10.1177/0309132517735706>

- Brignull, H. (2021). Bringing dark patterns to light: Transcript of the speech I gave at the Federal Trade Commission's Dark Patterns workshop on April 29, 2021. *Medium*. <https://harrybr.medium.com/bringing-dark-patterns-to-light-d86f24224ebf>
- Browne, S. (2015). *Dark Matters: On the Surveillanace of Blackness*. Duke University Press.
- Burgess, M. (2023, 16 May). How to boost WhatsApp's privacy and better protect your data. *Wired*. <https://www.wired.com/story/whatsapp-privacy-security-settings/#:~:text=Automatically%20collected%2C%20WhatsApp%20says%2C%20is,when%20you%20were%20last%20online>
- Burman, A. (2023). Understanding India's new data protection law. *Carnegie Endowment for International Peace, Carnegie India Working Paper*. <https://carnegieendowment.org/research/2023/10/understanding-indias-new-data-protection-law?lang=en>
- Butalia, U. (1993). Community, state and gender: On women's agency during partition. *Economic and Political Weekly*, 28(17), WS12–WS24. <http://www.jstor.org/stable/4399641>
- Carey, J. W. (2005). Historical pragmatism and the Internet. *New Media & Society*, 7(4), 443–455.
- Carey, J. W. and Quirk, J. J. (1989). The history of the future. In J. W. Carey (Ed) *Communication as culture (Revised edition)* (pp 485–503). John Wiley and Sons.
- Carmi, E. (2021). A feminist critique of digital consent. *Seminar.net*, 17(2). <https://doi.org/10.7577/seminar.4291>
- Carsten, J. (2004). *After Kinship*. Cambridge University Press.
- Carugati, C. (2023). The antitrust privacy dilemma. *European Competition Journal*, 19(2), 167–190. <https://doi.org/10.1080/17441056.2023.2169310>
- Cathcart, W. (2019, 29 October). Why WhatsApp is pushing back on NSO group hacking. *The Washington Post*.
- Cavoukian, A. (2010). Privacy by design: The 7 foundational principles implementation and mapping of fair information practices. <https://www.ipc.on.ca/en/media/1826/download?attachment>
- CCI (2024, 18 November). CCI imposes a monetary penalty of Rs. 213.14 crore on Meta for anti-competitive practices in relation to 2021 Privacy Policy Update. (Press Release No. 71/2024–25). <https://www.cci.gov.in/images/pressrelease/en/press-release1731941985.pdf>
- Ceci, L. (2024, 27 August). Number of unique WhatsApp mobile users worldwide from January 2020 to June 2024 (in millions). *Statista*. <https://www.statista.com/statistics/1306022/whatsapp-global-unique-users/>
- Cesarino, L. (2019). On digital populism in Brazil. *PoLAR: Political and Legal Anthropology Review*. <https://polarjournal.org/2019/04/15/on-jair-bolsonaros-digital-populism/>
- Chaitanya Rohilla v Union of India & Others*, Law Beat, High Court of Delhi (2021).

- Chakrabarti, S., Stengel, L. and Solanki, S. (2018). Duty, identity, credibility: Fake news and the ordinary citizen in India. BBC News. <https://downloads.bbc.co.uk/mediacentre/duty-identity-credibility.pdf>
- Chamorro-Premuzic, T. (2014). The distraction economy: How technology downgraded attention. *The Guardian*. <https://www.theguardian.com/media-network/media-network-blog/2014/dec/15/distraction-economy-technology-downgraded-attention-facebook-tinder>
- Chan, A. S. (2014). *Networking Peripheries: Technological Futures and the Myth of Digital Universalism*. MIT Press.
- Chatterjee, P. (1993). *The Nation and Its Fragments: Colonial and Postcolonial Histories*. Princeton University Press.
- Chaturvedi, A. (2020, 4 July). WhatsApp rolls out ‘It’s Between You’ campaign, narrates stories about how Indians communicate daily. *The Economic Times*.
- Chaudhuri, R. (2023). Decoding the G20 Consensus on Digital Public Infrastructure: A Key Outcome of India’s Presidency. *Carnegie India, Issue*. https://carnegieendowment.org/research/2023/09/decoding-the-g20-consensus-on-digital-public-infrastructure-a-key-outcome-of-indias-presidency?utm_source=chatgpt.com&lang=en
- Chaudhuri, R. and Kang Joseph, A. (2024). Living in a fragmented world: India’s data way. *India Review*, 23(2), 154–176.
- Cheeseman, N., Fisher, J., Hassan, I. and Hitchen, J. (2020). Social media disruption: Nigeria’s WhatsApp politics. *Journal of Democracy*, 31(3), 145–159.
- Chowdhury, N. (2018). Privacy and citizenship in India: Exploring constitutional morality and data privacy. *NUJS Law Review*, 11(3), 421–468.
- Chundru, A. (2021, 8 March). IT Rules 2021: CEO Will Cathcart says WhatsApp hopes to find solution to traceability without breaking encryption. *Medianama*. <https://www.medianama.com/2021/03/223-whatsapp-ceo-will-cathcart-traceability-it-rules-2021-2/>
- Citron, D. K. (2022). *The Fight for Privacy: Protecting Dignity, Identity, and Love in the Digital Age*. Chatto & Windus.
- Cohen, J. E. (2019a). *Between Truth and Power: The Legal Constructions of Informational Capitalism*. Oxford University Press.
- Cohen, J. E. (2019b). Review of Zuboff’s the age of surveillance capitalism: The fight for a human future at the new frontier of power. *Surveillance & Society*, 17(1/2), 240–245. <http://library.queensu.ca/ojs/index.php/surveillance-and-society/index>
- Competition Commission of India (2002). The Competition Act, 2002 (Act No. 12 of 2003). *India Code/CCI*.
- Competition Commission of India *Suo Moto Case No. 01* (March 24, 2021).
- Cornish, C. (2023, 11 October). India has embraced WhatsApp, but Meta now needs to make it pay. *Financial Times*. <https://www.ft.com/content/421f3766-656d-4890-8963-1851132be5e9>

- Couldry, N. and Mejias, U. A. (2023). The decolonial turn in data and technology research: what is at stake and where is it heading? *Information, Communication & Society*, 26(4), 786–802. <https://doi.org/10.1080/1369118X.2021.1986102>
- Couldry, N. and Mejias, U. A. (2019). *The Costs of Connection: How Data Is Colonizing Human Life and Appropriating It for Capitalism*. Stanford University Press.
- Cranor, L. F. (2012). Necessary but not sufficient: Standardized mechanisms of privacy notice and choice. *Journal on Telecommunications and High Technology Law*, 10, 273–307.
- Cruz-Moya, O. and Harindranath, R. (2020). WhatsApp as ‘technology of life’: Reframing research agendas. *First Monday*, 25(12). <https://doi.org/https://doi.org/10.5210/fm.v25i12.10405>
- Curato, N. and Fossati, D. (2020). Authoritarian innovations: Crafting support for a less democratic Southeast Asia. *Democratization*, 27(6), 1006–1020. <https://doi.org/https://doi.org/10.1080/13510347.2020.1777985>
- D’Cruze, D. (2024, 19 March). Pakistanis, UAE citizens get WhatsApp message from Indian IT Ministry’s ‘Viksit Bharat Sampark’ account. *Business Today*. <https://www.businesstoday.in/technology/news/story/pakistani-uae-citizens-get-whatsapp-message-from-indian-it-ministrys-viksit-bharat-sampark-account-422021-2024-03-19>
- Danaher, J. (2022). Techno-optimism: An analysis, an evaluation and a modest defence. *Philosophy & Technology*, 35(2), 54. <https://doi.org/10.1007/s13347-022-00550-2>
- Datta, A. (2018). The digital turn in postcolonial urbanism: Smart citizenship in the making of India’s 100 smart cities. *Transactions of the Institute of British Geographers*, 43(3), 405–419. <https://doi.org/https://doi.org/10.1111/tran.12225>
- Dattani, K. (2019). ‘Govrentrepreneurism’ for good governance: The case of Aadhaar and the India Stack. *Area*, 52(2), 411–419.
- Daub, A. (2020). *What Tech Calls Thinking: An Inquiry into the Intellectual Bedrock of Silicon Valley*. Farrar, Straus and Giroux ebook.
- Davenport, T. H. and Beck, J. C. (2001). *The Attention Economy: Understanding the New Currency of Business*. Harvard Business School Press.
- De, A. (2024). A Situated-Infrastructuring of WhatsApp for Business in India. In Extended Abstracts of the CHI Conference on Human Factors in Computing Systems (CHI EA ’24). 22: 1–7. Association for Computing Machinery, New York, NY, USA. <https://doi.org/10.1145/3613905.3651034>
- De, A. (2025). ‘Business on WhatsApp is tough now – but am I really a businesswoman?’ Exploring Challenges with Adapting to Changes in WhatsApp Business. In Proceedings of the 2025 CHI Conference on Human Factors in Computing Systems (CHI ’25). 967: 1–18. Association for Computing Machinery. <https://doi.org/10.1145/3706598.3713988>
- de Souza, P. S., Mukiri Smith, H. and Taylor, L. (2024). Decolonial Data Law and Governance. *Technology and Regulation*, 2024, 1–11.

- DeCew, J. W. (1997). *In Pursuit of Privacy: Law, Ethics, and the Rise of Technology*. Cornell University Press.
- Delaney, D. (2015). Legal geography I: Constitutivities, complexities, and contingencies. *Progress in Human Geography*, 39(1), 96–102.
- Dittmer, J. (2014). Geopolitical assemblages and complexity. *Progress in Human Geography*, 38(3), 385–401. <https://doi.org/10.1177/0309132513501405>
- Dixon, D. P. (2015). *Feminist Geopolitics Material States*. Routledge.
- Dixon, N. (2017). Stranger-ness and belonging in a neighbourhood WhatsApp Group. *Open Cultural Studies*, 1(1), 493–503. <https://doi.org/10.1515/culture-2017-0046>
- Dourish, P. and Mainwaring, S. D. (2012). Ubicomp's colonial impulse. *Proceedings of the 2012 ACM Conference on Ubiquitous Computing, Pittsburgh, Pennsylvania*. <https://doi.org/10.1145/2370216.2370238>
- Dowler, L. and Sharp, J. (2001). A feminist geopolitics? *Space and Polity*, 5(3), 165–176. <https://doi.org/10.1080/13562570120104382>
- Draper, N. A., Pieter Hoffmann, C., Lutz, C., Ranzini, G. and Turow, J. (2024). Privacy resignation, apathy, and cynicism: Introduction to a special theme. *Big Data & Society*, 11(3), 1–9. <https://doi.org/10.1177/20539517241270663>
- Durand, C. (2024). *How Silicon Valley Unleashed Techno-feudalism: The Making of the Digital Economy*. Verso.
- Dwoskin, E. (2018, 13 April). WhatsApp founder plans to leave after broad clashes with parent Facebook. *The Washington Post*. https://www.washingtonpost.com/business/economy/whatsapp-founder-plans-to-leave-after-broad-clashes-with-parent-facebook/2018/04/30/49448dd2-4ca9-11e8-84a0-458a1aa9ac0a_story.html
- Economic Times (2023). WhatsApp users can now avoid spam calls, thanks to 'Silence Unknown Caller' feature. https://economictimes.indiatimes.com/magazines/panache/whatsapp-users-can-now-avoid-spam-calls-thanks-to-silence-unknown-caller-feature/articleshow/101183215.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst
- Elkind, P., Gillum, J. and Silverman, C. (2021, 7 September). How Facebook undermines privacy protections for its 2 billion WhatsApp users. *ProPublica*. <https://www.propublica.org/article/how-facebook-undermines-privacy-protections-for-its-2-billion-whatsapp-users>
- Elwood, S. and Leszczynski, A. (2011). Privacy, reconsidered: New representations, data practices, and the geoweb. *Geoforum*, 42(1), 6–15. <https://doi.org/10.1016/j.geoforum.2010.08.003>
- Elwood, S. and Leszczynski, A. (2018). Feminist digital geographies. *Gender, Place & Culture*, 25(5), 629–644. <https://doi.org/10.1080/0966369X.2018.1465396>

- Enloe, C. (1989). *Bananas, Beaches and Bases: Making Feminist Sense of International Politics*. Rivers Oram Press/Pandora List.
- Escobar, A. (2017). *Designs for the Pluriverse: Radical Interdependence, Autonomy, and the Making of Worlds*. Duke University Press. <https://www.dukeupress.edu/designs-for-the-pluriverse>
- Eubanks, V. (2018). *Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor*. St. Martin's Press.
- European Commission. (2014a, 3 October). Mergers: Commission approves acquisition of WhatsApp by Facebook. https://ec.europa.eu/commission/presscorner/detail/en/ip_14_1088
- European Commission. (2014b, 3 October). Commission Decision of 3 October 2014 declaring a concentration to be compatible with the common market (Case No COMP/M.7217 – FACEBOOK / WHATSAPP) [EUR-Lex document 32014M7217, Official Journal L27/1].
- European Commission. (2017). Mergers: Commission fines Facebook €110 million for providing misleading information about WhatsApp takeover. https://ec.europa.eu/commission/presscorner/detail/en/ip_17_1369
- Evangelista, R. and Bruno, F. (2019). WhatsApp and political instability in Brazil: targeted messages and political radicalisation. *Internet Policy Review*, 8(4). <https://doi.org/10.14763/2019.4.1434>
- Facebook. (2014a). Discussion on acquisition of WhatsApp conference call. *Zuckerberg Transcripts*, 242. https://epublications.marquette.edu/zuckerberg_files_transcripts/242
- Facebook. (2014b). Facebook Q3 2014 Earnings Call. *Zuckerberg Transcripts*, 153. https://epublications.marquette.edu/zuckerberg_files_transcripts/153
- Facebook. (2015). Facebook Q3 2015 Earnings Call. *Zuckerberg Transcripts*, 232.
- Facebook. (2018a). 3rd Quarter and full year Earnings Call. *Meta Investor Relations*. <https://investor.atmeta.com/investor-news/press-release-details/2018/Facebook-Reports-Third-Quarter-2018-Results/default.aspx>
- Facebook. (2018b). Earnings Call Transcript Quarter 4. *Meta Investor Relations*. <https://investor.atmeta.com/investor-events/event-details/2019/Facebook-Q4-2018-Earnings/default.aspx>
- Facebook. (2020). Third Quarterly 2020 Results Conference Call. *Meta Investor Relations*. <https://investor.atmeta.com/investor-news/press-release-details/2020/Facebook-Reports-Third-Quarter-2020-Results/default.aspx>
- Facebook. (2021). Facebook Q4 Earnings Call. *Zuckerberg Transcripts*, 1506. https://epublications.marquette.edu/zuckerberg_files_transcripts/1506
- Farrow, R. (2022, 18 April). How democracies spy on their citizens. <https://www.newyorker.com/magazine/2022/04/25/how-democracies-spy-on-their-citizens>
- Fazal, T. (2016). *Practices of the State: Muslims, Law and Violence in India*. Three Essays Collective.

- Finextra. (2025). WhatsApp Pay made available to all Indian users. <https://www.finextra.com/newsarticle/45256/whatsapp-pay-made-available-to-all-indian-users>
- Flore, E. (2015, 29 June). 5 things you can learn from the story of WhatsApp. *Medium*. <https://medium.com/the-story-of-grip/5-things-every-founder-can-learn-from-the-story-of-whatsapp-b6496bc4f54d>
- Flyverbom, M. (2022). Overlit: Digital architectures of visibility. *Organization Theory*, 3(3), 1–16. <https://doi.org/10.1177/26317877221090314>
- Foer, F. (2017, 19 September). Facebook's war on free will. *The Guardian*. <https://www.theguardian.com/technology/2017/sep/19/facebooks-war-on-free-will?ref=cyberlaw.stanford.edu>
- Fortier, A.-M. (2010). Proximity by design? Affective citizenship and the management of unease. *Citizenship Studies*, 14(1), 17–30. <https://doi.org/10.1080/13621020903466258>
- Frampton, K. (2001). *Studies in Tectonic Culture: The Poetics of Construction in Nineteenth and Twentieth Century Architecture*. MIT Press.
- Frenkel, S. and Kang, C. (2021). *An Ugly Truth: Inside Facebook's Battle for Domination*. Bridge Street Press.
- Frew, S. (nd). Back to basics: What is the meaning of 'tectonic' in architecture today? *Architizer*. <https://architizer.com/blog/inspiration/stories/meaning-of-tectonic-in-architecture-today/>
- Froomkin, M. (1995). The metaphor is the key: Cryptography, the clipper chip, and the constitution. *University of Pennsylvania Law Review*, 143, 709–897.
- Fuchs, C. (2017). *Social Media: A Critical Introduction* (2nd ed). Sage Publications.
- Gajda, A. (2022). *Seek and Hide: The Tangled History of the Right to Privacy*. Viking.
- Gajjala, R. (2019). *Digital Diasporas: Labor and Affect in Gendered Indian Digital Publics*. Rowman & Littlefield.
- Gajjala, R. and Verma, T. (2018). Affect and relationality. In J. W. Morris and S. Murray (Eds) *Applied: Culture in the Age of Apps* (pp 205–215). University of Michigan Press.
- Gannes, L. (2013). WhatsApp CEO Jan Koum hates advertising and the tech rumor mill [Full Dive Video]. <https://allthingsd.com/20130510/whatsapp-ceo-jan-koum-hates-advertising-and-the-tech-rumor-mill-full-dive-video/index.html>
- Garimella, K. and Eckles, D. (2020). Images and misinformation in political groups: Evidence from WhatsApp in India [Preprint]. <https://arxiv.org/abs/2005.0978>
- Gebhart, G. (2016). *What Facebook and WhatsApp's Data Sharing Plans Really Mean for User Privacy*. Electronic Frontier Foundation. <https://www.eff.org/deeplinks/2016/08/what-facebook-and-whatsapps-data-sharing-plans-really-mean-user-privacy-0>

- Gehl, R. (2016). Power/freedom on the dark web: A digital ethnography of the Dark Web Social Network. *New Media & Society*, 18(7), 1219–1235. <https://doi.org/10.1177/1461444814554900>
- Gerbaudo, P. (2012). *Tweets and the Streets: Social Media and Contemporary Activism*. Pluto Press.
- Gill, L. (2018). Law, metaphor, and the encrypted machine. *Osgoode Hall Law Journal*, 55(2), 440–477. <https://doi.org/10.60082/2817-5069.3290>
- Gillespie, T. (2010). The politics of ‘platforms’. *New Media & Society*, 12(3), 347–364. <https://doi.org/10.1177/1461444809342738>
- Gonzalez, R. J. (2017). Hacking the citizenry? Personality profiling, big data, and the election of Donald Trump. *Anthropology Today*, 33(3), 9–12.
- Government of India. (2021). The government respects the right of privacy and has no intention to violate it when Whatsapp is required to disclose the origin of a particular message [Press release]. <https://www.pib.gov.in/PressReleasePage.aspx?PRID=1721915®=3&lang=2>
- Goyal, G. and Kumar, R. (2016). *The Right to Privacy in India: Concept and Evolution*. PartridgeIndia.
- Graham, S. (1998). The end of geography or the explosion of place? Conceptualizing space, place and information technology. *Progress in Human Geography*, 22(2), 165–185.
- Graham, S. and Marvin, S. (2001). *Splintering Urbanism: Networked Infrastructures, Technological Mobilities and the Urban Condition* (1st ed). Routledge. <https://doi.org/10.4324/9780203452202>
- Gratton, P. (2024). How WhatsApp makes money. *Investopedia.com*. <https://www.investopedia.com/articles/personal-finance/040915/how-whatsapp-makes-money.asp#:~:text=Click%2Dto%2DWhatsApp%20Ads,bill%20in%20revenue%20in%202024>
- Green, J. (2014). *Rethinking Private Authority: Agents and Entrepreneurs in Global Environmental Governance*. Princeton University Press.
- Habermas, J. R. (2005). *The Theory of Communicative Action: A Critique of Functionalist Reason*. Beacon.
- Hall, R. B. and Biersteker, T. J. (2002). The emergence of private authority in international system. In *The Emergence of Private Authority in Global Governance* (pp 3–22). Cambridge University Press.
- Haraway, D. (1985). *A Cyborg Manifesto: Science, Technology, and Socialist-Feminism in the Late Twentieth Century*. Routledge.
- Haraway, D. (1988). Situated knowledges: The science question in feminism and the privilege of partial perspective. *Feminist Studies*, 14(3), 575–599.
- Haraway, D. (2004). *The Haraway Reader*. Routledge.
- Hargittai, E. and Marwick, A. (2016). ‘What can I really do?’ Explaining the privacy paradox with online apathy. *International Journal of Communication*, 10, 3737–3757.

- Harriss, J. (2006). Middle-class activism and the politics of the informal working class. *Critical Asian Studies*, 38(4), 445–465. <https://doi.org/10.1080/14672710601073002>
- Harsha Gupta v WhatsApp LLC & Ors.* Delhi High Court (2021).
- Hartman, T. K., Stocks, T. V. A., McKay, R., Gibson-Miller, J., Levita, L., Martinez, A. P. et al (2021). The authoritarian dynamic during the COVID-19 pandemic: Effects on nationalism and anti-immigrant sentiment. *Social Psychological and Personality Science*, 12(7), 1274–1285. <https://doi.org/10.1177/1948550620978023>
- Hassan, I. and Hitchen, J. (Eds) (2022). *WhatsApp and Everyday Life in West Africa: Beyond Fake News*. Bloomsbury Publishing.
- Haupt, J. (2021). Facebook futures: Mark Zuckerberg’s discursive construction of a better world. *New Media & Society*, 23(2), 237–257. <https://doi.org/10.1177/1461444820929315>
- Heidegger, M. (1977 [1954]). *The Question Concerning Technology and Other Essays* (Translated and with an Introduction by W. Lovitt). Garland Publishing, Inc.
- Hern, A. (2021). WhatsApp loses millions of users after terms update. *Guardian*. <https://www.theguardian.com/technology/2021/jan/24/whatsapp-loses-millions-of-users-after-terms-update>
- Hindu Bureau. (2024, 21 March). EC asks MeITY to stop Viksit Bharat messages. *The Hindu*.
- Hitchen, J., Hassan, I., Fisher, J. and Cheeseman, N. (2019). *WhatsApp and Nigeria’s 2019 Elections: Mobilising the People, Protecting the Vote*. <https://www.cddwestafrica.org/reports/whatsapp-and-nigeria-s-2019-elections-mobilising-the-people-protesting-the-vote/>
- Hoepman, J.-H. (2021). *Privacy Is Hard and Seven Other Myths*. MIT Press.
- Hoffmann, A. L., Proferes, N. and Zimmer, M. (2018). ‘Making the world more open and connected’: Mark Zuckerberg and the discursive construction of Facebook and its users. *New Media & Society*, 20(1), 199–218. <https://doi.org/10.1177/1461444816660784>
- Horst, H. A. and Miller, D. (Eds) (2012). *Digital Anthropology* (1st ed). Routledge. <https://doi.org/https://doi.org/10.4324/9781003085201>
- Horst, H. A., Miller, D. and Taylor & Francis. (2013). *Digital Anthropology* (1st ed). Bloomsbury Publishing. <http://UCL.ebib.com/patron/FullRecord.aspx?p=1274330>
- Hyndman, J. (2004). Mind the gap: Bridging feminist and political geography through geopolitics. *Political Geography*, 23(3), 307–322.
- Hyndman, J. (2019). Unsettling feminist geopolitics: Forging feminist political geographies of violence and displacement. *Gender, Place & Culture*, 26(1), 3–29. <https://doi.org/10.1080/0966369X.2018.1561427>
- Igo, S. E. (2018). *The Known Citizen: A History of Privacy in Modern America*. Harvard University Press.

- INCKerala [X]. (2024, 16 March). <https://x.com/INCKerala/status/1768933455604371934>
- IndBiz. (2018). Invest India, WhatsApp to promote startups. <https://indbiz.gov.in/invest-india-whatsapp-to-promote-startups/>
- India Today Tech. (2021, 16 January). After backlash, WhatsApp delays new privacy policy says ‘giving more time for our recent update’. *India Today*. <https://www.indiatoday.in/technology/news/story/after-backlash-whatsapp-delays-new-privacy-policy-says-giving-more-time-for-our-recent-update-1759585-2021-01-16>
- Ingold, T. (2005). Towards a politics of dwelling. *Conservation and Society*, 3(2), 501–508.
- Isin, E. and Ruppert, E. (2019). Data’s Empire: Postcolonial data politics. In D. Bigo, E. Isin and E. Ruppert (Eds) *Data Politics: Worlds, Subjects, Rights* (pp 207–227). Routledge.
- Isin, E. and Ruppert, E. (2020). *Being Digital Citizens*. Bloomsbury.
- Issac, M. (2023, 8 November). Mark Zuckerberg taps the strengths of WhatsApp. *New York Times*.
- Jackman, A. and Brickell, K. (2022). ‘Everyday droning’: Towards a feminist geopolitics of the drone-home. *Progress in Human Geography*, 46(1), 156–178. <https://doi.org/10.1177/03091325211018745>
- Jaffrelot, C. (translated by Cynthia Schoch) (2021). *Modi’s India: Hindu Nationalism and the Rise of Ethnic Democracy*. Princeton University Press.
- Jaffrelot, C. and Verniers, G. (2020). The BJP’s 2019 election campaign: not business as usual. *Contemporary South Asia*, 28(2), 155–177. <https://doi-org.ezproxy.library.qmul.ac.uk/10.1080/09584935.2020.1765985>
- Jasanoff, S. and Kim, S.-H. (Eds) (2015). *Dreamscapes of Modernity: Sociotechnical Imaginaries and the Fabrication of Power*. University of Chicago Press.
- Jaswal, S. (2024). Inside the BJP’s WhatsApp machine. <https://restofworld.org/2024/bjp-whatsapp-modi/>
- Jazeel, T. (2016). Between area and discipline: Progress, knowledge production, and the geographies of Geography. *Progress in Human Geography*, 40(5), 649–667.
- Jazeera, A. (2021, 14 January). WhatsApp battles privacy concerns in India – its biggest market. *Al Jazeera*. <https://www.aljazeera.com/news/2021/1/14/whatsapp-battles-privacy-concerns-in-india-its-biggest-market>
- Jeffrey, A. (2019). *The Edge of Law: Legal Geographies of a War Crimes Court*. Cambridge University Press. <https://doi.org/10.1017/9781108186018>
- John, N. (2024). Sharing and social media: The decline of a keyword? *New Media & Society*, 26(4), 1891–1908. <https://doi.org/10.1177/14614448221078603>
- John, N. A. (2012). Sharing and Web 2.0: The emergence of a keyword. *New Media & Society*, 15(2), 167–182. <https://doi.org/10.1177/1461444812450684>

- Johns, A. and Cheong, N. (2021). The affective pressures of WhatsApp: From safe spaces to conspiratorial publics. *Journal of Media & Cultural Studies*, 35(5), 732–746. <https://doi.org/https://doi.org/10.1080/10304312.2021.1983256>
- Johns, A., Matamoros-Fernández, A. and Baulch, E. (2023). *WhatsApp: From a One-to-one Messaging App to a Global Communication Platform*. John Wiley and Sons Ltd.
- Kamra, L. and Khatri, S. (2021). The pandemic in the periphery of Delhi: COVID-19 and boundary (re)making in peri-urban India. *City & Society*, 33(2), 283–302. <https://doi.org/https://doi.org/10.1111/ciso.12332>
- Kamra, L., Williams, P. and Johar, P. (2023). Grassroots authoritarianism: WhatsApp, middle-class boundary-making and pandemic governance in New Delhi's neighbourhoods. *Territory, Politics, Governance*, 11(6), 1121–1140. <https://doi.org/10.1080/21622671.2022.2160372>
- Kannabiran, K. and Ballakrishnen, S. S. (2021). *Gender Regimes and the Politics of Privacy: A Feminist Re-reading of Puttaswamy v Union of India*. Zubaan.
- Kantrowitz, A. (2022, 5 March). WhatsApp head Will Cathcart dishes on Signal, India, and Apple. *Medium.com*. <https://onezero.medium.com/whatsapp-head-will-cathcart-dishes-on-signal-india-and-apple-db81b4553718>
- Karmanya Singh Sareen & Anr v Union of India*, High Court of New Delhi (2016).
- Karmanya Singh Sareen & Anr v Union of India & Others Special Leave Petition*, Supreme Court of India (2017).
- Karp, P. (2018, 7 December). Australia's war on encryption: The sweeping new powers rushed into law. *Guardian*. <https://www.theguardian.com/technology/2018/dec/08/australias-war-on-encryption-the-sweeping-new-powers-rushed-into-law>
- Karusala, N., Bhalla, A. and Kumar, N. (2019). *Privacy, Patriarchy, and Participation on Social Media*. Proceedings of the 2019 on Designing Interactive Systems Conference. <https://doi.org/10.1145/3322276.3322355>
- Katz, C. (2001). On the grounds of globalization: A topography for feminist political engagement. *Signs*, 26(4), 1213–1234. <http://www.jstor.org/stable/3175362>
- Kelly, L. (1987). The continuum of sexual violence. In J. Hamner and M. Maynard (Eds) *Women, Violence and Social Control* (pp 46–60). Springer.
- Khaira, R. (2022, 8 March). How TrueCaller built a billion-dollar caller ID data empire in India. *Rest of World*. <https://restofworld.org/2022/how-truecaller-built-a-billion-dollar-id-data-empire-in-india/>
- Khanal, S., Zhang, H. and Taihagh, A. (2024). Why and how is the power of Big Tech increasing in the policy process? The case of generative AI. *Policy and Society*. <https://doi.org/10.1093/polsoc/puae012>

- Khatri, A. (2024). WhatsApp uncles | Stand-up comedy by Atul Khatri. <https://www.youtube.com/watch?v=u9TGbV8hr8s>
- Kini, S., Pathak-Shelat, M. and Jain, V. (2022). Conceptualizing ‘filtering’: Affordances, context collapse, and the social self online. *International Journal of Communication*, 16(2022), 1573–1593. <https://ijoc.org/index.php/ijoc/article/view/18388>
- Kitchin, R. and Dodge, M. (2011). *Code/Space: Software and Everyday Life*. MIT Press.
- Kleinman, Z. (2025, 21 February). Apple pulls data protection tool after UK government security row. *BBC News online*. <https://www.bbc.co.uk/news/articles/cgj54eq4vejo>
- Kumar, N. (2025a, 20 January). The privacy-antitrust paradox? Analysing the CCI’s penalty order against Meta and WhatsApp. Internet Freedom Foundation. <https://internetfreedom.in/the-privacy-antitrust-paradox-analysing-the-ccis-penalty-order-against-meta-and-whatsapp/#:~:text=On%2018%20November%202024%2C%20the,NCLAT%2C%20challenging%20the%20CCI’s%20jurisdiction>
- Kumar, N. (2025b). WhatsApp users statistics 2025: How many people use it? https://www.demandsage.com/whatsapp-statistics/?utm_source=chatgpt.com
- Kumar, R. (2024). *Electoral bonds in WhatsApp university*. [Video] YouTube. https://www.youtube.com/watch?v=4dFv_S9nJq4&ab_channel=RavishKumarOfficial
- Lakoff, G. (1993). The contemporary theory of metaphor. In A. Ortony (Ed), *In Metaphor and Thought* (2nd ed) (pp 202–251). Cambridge University Press. <https://doi.org/10.1017/CBO9781139173865.013>
- Lakoff, G. and Johnson, M. (1980). *Metaphors We Live By*. University of Chicago Press.
- Lapowsky, I. (2024, 9 December). How WhatsApp for Business changed the world. *Rest of the World*. <https://restofworld.org/2024/how-whatsapp-for-business-changed-the-world/>
- Legg, S. (2003). Gendered politics and nationalised homes: Women and the anti-colonial struggle in Delhi, 1930–47. *Gender, Place, and Culture*, 10(1), 7–27.
- Lessig, L. (2002). Privacy as property. *Social Research*, 69(1), 247–269.
- Leszczynski, A. (2020). Digital methods III: The digital mundane. *Progress in Human Geography*, 44(6), 1194–1201. <https://doi.org/10.1177/0309132519888687>
- Levy, S. (2020). *Facebook: The Inside Story*. Penguin Random House.
- Lewis, H. (2021, 5 October). What happened when Facebook became Boomerbook. *Atlantic*. <https://www.theatlantic.com/ideas/archive/2021/10/facebook-midlife-crisis-boomerbook/620307/>

- Livemint. (2019, 2 January). India's data must be controlled by Indians: Mukesh Ambani. *Livemint*. <https://www.livemint.com/Companies/QMZDxbCufK3O2dJE4xccyI/Indias-data-must-be-controlled-by-Indians-not-by-global-co.html>
- Livemint. (2025, 28 August). Delhi Government mulls 'WhatsApp Governance' for Public Services. *Livemint*. <https://www.livemint.com/news/india/delhi-govt-mulls-whatsapp-governance-for-public-services-get-driving-licence-and-marriage-certificates-instantly-11756347344309.html>
- LocalCircles. (2025). 87% citizens surveyed say their personal data already stands compromised with 50% concerned about their Aadhaar details; Most hold telcos, eCommerce. <https://www.localcircles.com/a/press/page/personal-data-leakage>
- Lochab, H. (2025). WhatsApp ads will not bother most users, privacy stays intact, assures head Will Cathcart. *The Economic Times*.
- Locke, J. (Ed). (1690). *Second Treatise on Government*. Macmillan, Library of Liberal Arts.
- Lorimer, H. (2005). Cultural geography: The busyness of being 'more-than-representational'. *Progress in Human Geography*, 29(1), 83–94. <https://doi.org/10.1191/0309132505ph531pr>
- Lyon, D. (2001). *Surveillance Society: Monitoring Everyday Life*. Open University Press.
- Lyon, D. (2018). *The Culture of Surveillance: Watching as a Way of Life*. Polity.
- MacKinnon, C. A. (1989). *Toward a Feminist Theory of the State*. Harvard University Press.
- Manohar Lal Sharma v Union of India*, Supreme Court of India (2021).
- Markham, T. and ProQuest, P. (2020). *Digital life*. Polity.
- Marston, S. A., Jones III, J. P. and Woodward, K. (2005). Human geography without scale. *Transactions of the Institute of British Geographers*, 30(4), 416–432.
- Marwick, A. (2022). Privacy without power: What privacy research can learn from surveillance studies. *Surveillance & Society*, 20(4), 397–405.
- Marwick, A. (2023). *The Private Is Political: Networked Privacy and Social Media*. Yale University Press. <https://doi.org/9780300229622>
- Marwick, A. E. and boyd, d. (2011). I tweet honestly, I tweet passionately: Twitter users, context collapse, and the imagined audience. *New Media & Society*, 13(1), 114–133. <https://doi.org/10.1177/1461444810365313>
- Masiero, S. (2022). Decolonising critical information systems research: A subaltern approach. *Information Systems Journal*, 33(2), 299–323.
- Matthan, R. (2018). *Privacy 3.0: Unlocking Our Data-driven Future*. Harper Collins.
- Mayer, J., Mutchler, P. and Mitchell, J. C. (2016). Evaluating the privacy properties of telephone metadata. *PNAS*, 113(20), 5536–5541. <https://doi.org/10.1073/pnas.1508081113>

- McCallum, S. (2022). WhatsApp: We won't lower security for any government. *BBC News online*. <https://www.bbc.co.uk/news/technology-62291328>
- McDonald, A. M. and Cranor, L. F. (2008). The cost of reading privacy policies. *I/S: A Journal of Law and Policy for the Information Society*, 4(3 Winter 2008/2009), 543–568. <https://doi.org/2015-09-30T22:41:07Z>
- McDonald, T. (2015). Affecting relations: Domesticating the internet in a south-western Chinese town. *Information, Communication & Society*, 18(1), 17–31.
- McDowell, L. (1993). Space, place, and gender relations, Part I: Feminist empiricism and the geography of social relations. *Progress in Human Geography*, 17(2), 157–179.
- McGlotten, S. (2016). Black data. In P. Johnson (Ed) *No Tea, No Shade: New Writings in Black Queer Studies*. Duke University Press.
- McLaughlin, T. (2018, 12 December). How WhatsApp fuels fake news and violence in India. *Wired*. <https://www.wired.com/story/how-whatsapp-fuels-fake-news-and-violence-in-india/>
- McNamee, R. (2019). *Zucked: Waking Up to the Facebook Catastrophe*. Harper Collins.
- Meinrath, S. D., Losey, J. W. and Pickard, V. W. (2011). Digital feudalism: Enclosures and erasures from digital rights management to the digital divide. In M. V. Zelkowitz (Ed), *Advances in Computers* (Vol. 81, pp 237–287). Elsevier. <https://doi.org/https://doi.org/10.1016/B978-0-12-385514-5.00005-7>
- Menon, N. (2022). *Seeing like a Feminist*. Zubaan.
- Mertia, S. (Ed) (2020). *Lives of Data: Essays on Computational Cultures from India*. Institute of Network Cultures.
- Meta. (2023a, 23 August). Highlighting WhatsApp's privacy features at Mumbai's iconic gateway of India. <https://about.fb.com/news/2023/08/highlighting-whatsapps-privacy-features-at-mumbais-iconic-gateway-of-india/>
- Meta. (2023b). Supporting small businesses to unlock the power of digital commerce. <https://about.fb.com/news/2023/12/supporting-small-businesses-to-unlock-the-power-of-digital-commerce/>
- Meta. (2024). Earnings call Quarter 4. https://s21.q4cdn.com/399680738/files/doc_financials/2024/q4/META-Q4-2024-Earnings-Call-Transcript.pdf
- Meta Developers. (2019). F8 2019 day 1 keynote. [Video] YouTube. <https://www.youtube.com/watch?v=xK0RwubFi-U>
- Meta Platforms. (2024). *Second Quarter 2024 Results Conference Call*. https://s21.q4cdn.com/399680738/files/doc_financials/2024/q2/META-Q2-2024-Earnings-Call-Transcript.pdf
- Meta Platforms, Inc. v Competition Commission of India*, National Company Law Appellate Tribunal, 4 November 2025.

- Michelutti, L. (2007). The vernacularisation of democracy: Political participation and popular politics in North India. *Journal of the Royal Anthropological Institute*, 13(3), 639–656.
- Mihindukulasuriya, R. (2021, 20 January). Are Indians worried about privacy? Not really, shows data on WhatsApp, Signal, Telegram usage. *The Print*. <https://theprint.in/tech/are-indians-worried-about-privacy-not-really-shows-data-on-whatsapp-signal-telegram-usage/588276/>
- Milan, S. and Treré, E. (2019). Big Data from the South(s): Beyond data universalism. *Television & New Media*, 20(4), 319–335.
- Ministry of Electronics and Information Technology. (2019). About digital India. <https://www.digitalindia.gov.in>
- Ministry of Electronics and Information Technology. (2021). The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021. Government of India. <https://prsindia.org/billtrack/the-information-technology-intermediary-guidelines-and-digital-media-ethics-code-rules-2021>
- Monahan, T. (2017). Regulating belonging: Surveillance, inequality, and the cultural production of abjection. *Journal of Cultural Economy*, 10(2), 191–206. <https://doi.org/10.1080/17530350.2016.1273843>
- Morley, D. and Silverstone, R. (1990). Domestic communication: Technologies and meanings. *Media, Culture, and Society*, 12(1), 31–55.
- Mountz, A. and Hyndman, J. (2006a). Feminist approaches to the global intimate. *Women's Studies Quarterly*, 34(1/2), 446–463. <http://www.jstor.org/stable/40004773>
- Mountz, A. and Hyndman, J. (2006b). Feminist approaches to the global intimate. *Women's Studies Quarterly*, 34(1), 446–463.
- Mohamed, S., Png, M-T and Isaac, W. (2020). Decolonial AI: Decolonial theory as sociotechnical foresight in artificial intelligence. *Philosophy & Technology* 33, 659–684.
- Mukerjee, S. (2016). Net neutrality, Facebook, and India's battle to #SaveTheInternet. *Communication and the Public*, 1(3), 356–361. <https://doi.org/10.1177/2057047316665850>
- Murphy, H. and Findlay, S. (2020, 6 November). WhatsApp gets green light to launch payments service in India. *Financial Times*. <https://www.ft.com/content/b72efc94-8dd4-439f-8081-6392020b4438>
- Nanda, A. S. (2024, 6 February). Pioneering privacy: Understanding the essence and impact of privacy by design. *Medianama*. <https://www.medianama.com/2024/02/223-dpdp-act-understanding-privacy-by-design-2/>
- Narayan, S. S. and Narayanan, S. (2024). *The WhatsApp India Story: Inside the Digital Maya Sphere*. Routledge.

- Neate, R. (2020, 10 December). Facebook faces biggest legal battle in years as US officials launch lawsuits. <https://www.theguardian.com/technology/2020/dec/10/facebook-faces-biggest-legal-battle-in-years-as-us-officials-launch-lawsuits>
- New York Times. (2021). WhatsApp delays privacy changes amid user backlash. *The New York Times*. <https://www.nytimes.com/2021/01/15/technology/whatsapp-privacy-changes-delayed.html>
- Newton, C. (2021, 14 September). WhatsApp CEO Will Cathcart on a rocky year for the app. *The Verge*. <https://www.theverge.com/2021/9/13/22672756/whatsapp-ceo-will-cathcart-interview-2021-propublica-privacy-encryption>
- Nilekani, N. and Shah, V. (2016). *Rebooting India: Realizing a Billion Aspirations*. Allen Lane.
- Nippert-Eng, C. (2010). *Islands of Privacy*. University of Chicago Press.
- Nissenbaum, H. (2009). *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Imprint: Stanford Law Books.
- Nussbaum, M. C. (2000, 1 April). Is privacy bad for women? <https://www.bostonreview.net/articles/martha-c-nussbaum-privacy-bad-women/>
- Nyabola, N. (2018). *Digital Democracy, Analogue Politics: How the Internet Era is Transforming Politics in Kenya*. Zed Books.
- Olson, P. (2014a, 19 February). Exclusive: The rags-to-riches tale of how Jan Koum built WhatsApp into Facebook's new \$19 billion baby. *Forbes*. <https://www.forbes.com/sites/parmyolson/2014/02/19/exclusive-inside-story-how-jan-koum-built-whatsapp-into-facebooks-new-19-billion-baby/>
- Olson, P. (2014b, 4 March). Inside The Facebook: WhatsApp megadeal: The courtship, the secret meetings, the \$19 billion poker game. *Forbes*. <https://www.forbes.com/sites/parmyolson/2014/03/04/inside-the-facebook-whatsapp-megadeal-the-courtship-the-secret-meetings-the-19-billion-poker-game/>
- Olson, P. (2018, 26 September). Exclusive: WhatsApp cofounder Brian Acton gives the inside story on #DeleteFacebook and why he left \$850 million behind. *Forbes*. <https://www.forbes.com/sites/parmyolson/2018/09/26/exclusive-whatsapp-cofounder-brian-acton-gives-the-inside-story-on-deletefacebook-and-why-he-left-850-million-behind/>
- Omanga, D. (2019). WhatsApp as 'digital publics': The Nakuru Analysts and the evolution of participation in county governance in Kenya. *Journal of Eastern African Studies*, 13(1), 175–191.
- Omvedt, G. (2003). *Buddhism in India: Challenging Brahmanism and Caste*. Sage Publications.
- Ong, J. C., Tapsell, R. and Curato, N. (2019). Tracking digital disinformation in the 2019 Philippine midterm election (New Mandala, August 2019). <https://www.newmandala.org/wp-content/uploads/2019/08/Digital-Disinformation-2019-Midterms.pdf>

- Outlook. (2018, 31 October). Focused on simplicity, quality, security and privacy: WhatsApp vice president. *Outlook*. <https://www.outlookindia.com/national/focused-on-simplicity-quality-security-and-privacy-whatsapp-vice-president-news-319347>
- Outlook Web Bureau. (2019, 31 October). Indian activists, journalists hit by Israeli Spyware, govt seeks response from WhatsApp. *Outlook*. <https://www.outlookindia.com/national/india-news-govt-seeks-whatsapps-response-on-israeli-spyware-snooping-on-indian-activists-journalists-news-341452>
- Ovide, S. (2020, 1 December). Why WhatsApp matters. *The New York Times*. <https://www.nytimes.com/2020/12/01/technology/why-whatsapp-matters.html>
- Oza, E., Williams, P. and Kamra, L. (2024). Digital denizenship: Hindu nationalist architectures of digital closings and unbelonging in India. *Environment and Planning C: Politics and Space*, 42(7), 1150–1169. <https://doi.org/10.1177/23996544241226813>
- Page, C. (2021). WhatsApp tells users: Share your data with Facebook or we'll delete your account. *Forbes*. <https://www.forbes.com/sites/carlypage/2021/01/08/whatsapp-tells-users-share-your-data-with-facebook-or-well-deactivate-your-account/?sh=4e5dd3722d46>
- Pahuja, S. (2011). *Decolonising International Law: Development, Economic Growth and the Politics of Universality*. Cambridge University Press.
- Paley, J. (2002). Toward an anthropology of democracy. *Annual Review of Anthropology*, 31, 469–496.
- Pandey, G. (2005). *Routine Violence: Nations, Fragments, Histories*. Stanford University Press.
- Papacharissi, Z. (2010). *A Private Sphere: Democracy in a Digital Age*. Polity.
- Papacharissi, Z. (2014). *Affective Publics: Sentiment, Technology, and Politics*. Oxford University Press. <https://doi.org/10.1093/acprof:oso/9780199999736.001.0001>
- Parsheera, S. (2024). Stack is the new black?: Evolution and outcomes of the 'India-Stackification' process. *Computer Law & Security Review*, 52, Article 105947. <https://doi.org/https://doi.org/10.1016/j.clsr.2024.105947>
- Pasquale, F. A. (2013). Privacy, antitrust, and power. *George Mason Law Review, U of Maryland Legal Studies Research Paper No. 2013–44*, 20(4), 1009–1024.
- Pateman, C. (1988). *The Sexual Contract*. Stanford University Press.
- Pateman, C. (1989). *The Disorder of Women: Democracy, Feminism, and Political Theory*. Stanford University Press.
- Paul, K. (2022, 17 November). Meta's WhatsApp makes Brazil a key test market for business messaging. *Reuters*. <https://www.reuters.com/technology/metas-whatsapp-makes-brazil-key-test-market-business-messaging-2022-11-17/>

- Pereira, G., Bueno Bojczuk Camargo, I. and Parks, L. (2021). WhatsApp disruptions in Brazil: A content analysis of user and news media responses, 2015–2018. *Global Media and Communication*, 18(1), 113–148. <https://doi.org/10.1177/17427665211038530>
- Phadke, S., Khan, S. and Ranade, S. (2011). *Why Loiter? Women and Risk on Mumbai Streets*. Penguin Books.
- Phartiyal, S. (2018, 4 July). WhatsApp in India says partnership with government, society needed to combat misinformation. *Reuters*. <https://www.reuters.com/article/us-whatsapp-india-fakenews/whatsapp-in-india-says-partnership-with-government-society-needed-to-combat-misinformation-idUSKBN1JU0HO/>
- Philips, D. (2015, 17 December). Brazil's ban on WhatsApp is lifted less than 24 hours after it began. *The Washington Post*. [https://www.washingtonpost.com/news/worldviews/wp/2015/12/17/brazil-silences-whatsapp-mess age-service-for-48-hours-but-nothing-stops-the-outrage/](https://www.washingtonpost.com/news/worldviews/wp/2015/12/17/brazil-silences-whatsapp-mess-age-service-for-48-hours-but-nothing-stops-the-outrage/)
- PIB. (2018a). Whatsapp told to find more effective solutions. [Press release] Ministry of Electronics and Information Technology, *Government of India*. Delhi. <https://www.pib.gov.in/newsite/PrintRelease.aspx?relid=180787®=3&lang=2>
- PIB. (2018b). WhatsApp warned for abuse of their platform. [Press release] Ministry of Electronics and Information Technology, *Government of India*. Delhi. <https://www.pib.gov.in/newsite/PrintRelease.aspx?relid=180364®=3&lang=2>
- Pink, S., Horst, H., Postill, J., Hjorth, L., Lewis, T. and Tacchi, J. (2016). *Digital Ethnography: Principles and Practice*. SAGE Publications.
- Poggiali, L. (2016). Seeing (from) digital peripheries: Technology and transparency in Kenya's Silicon Savannah. *Cultural Anthropology*, 31(3), 387–411.
- Poggiali, L. (2017). Digital futures and analogue pasts? Citizenship and ethnicity in techno-utopian Kenya. *Africa: Journal of the International African Institute*, 87(2), 253–277. <http://www.jstor.org/stable/26158168>
- Pope, R. (2016). Software is politics. <https://www.fastcompany.com/3066631/software-is-politics>
- PTI. (2021, 19 May). IT ministry directs WhatsApp to withdraw new privacy policy: Government sources. *The Times of India*. <https://timesofindia.indiatimes.com/business/india-business/centre-reiterates-demand-for-withdrawal-of-whatsapps-new-privacy-policy/articleshowprint/82764544.cms>
- PTI. (2023, 1 February). Privacy policy: SC asks WhatsApp to publicise undertaking given to Centre in 2021. *Economic Times*. <https://economictimes.indiatimes.com/tech/technology/privacy-policy-sc-asks-whatsapp-to-publicise-undertaking-given-to-centre-in-2021/articleshow/97526969.cms?from=mdr>

- Purnell, N. (2018). The Internet is filling up because indians are sending millions of 'good morning!' texts. *The Wall Street Journal*. <https://www.wsj.com/articles/the-internet-is-filling-up-because-indians-are-sending-millions-of-good-morning-texts-1516640068>
- PWC. (2024). How aware and prepared are Indian consumers and businesses to navigate the new era of digital privacy? A survey of India's data privacy relandscape. <https://www.pwc.in/assets/pdfs/aware-prepared-indian-consumers-businesses-navigate-new-era-digital-privacy.pdf>
- Rajagopal, A. (2001). *Politics After Television: Hindu Nationalism and the Reshaping of the Indian Public*. Cambridge University Press.
- Rao, S. M. (2025, 30 January). Andhra Pradesh to roll out WhatsApp Governance. *The Hindu*. <https://www.thehindu.com/news/national/andhra-pradesh/andhra-pradesh-to-roll-out-whatsapp-governance-on-january-30/article69154772.ece>
- Rawls, J. (1971). *A Theory of Justice*. Cambridge University Press.
- Reed, C. and Murray, A. (2018). *Rethinking the Jurisprudence of Cyberspace*. Edward Elgar Publishing. <https://doi.org/10.4337/9781785364297>
- Reidenberg, J. R., Breaux, T., Cranor, L. F., French, B. M., Grannis, A., Graves, J. T. et al (2015). Disagreeable privacy policies: Mismatches between meaning and users' understanding. *Berkeley Tech. L. J.*, 39. https://ir.lawnet.fordham.edu/faculty_scholarship/619
- Rennó, R. (2018). WhatsApp: The widespread use of WhatsApp in political campaigning in the global south, *Tactical Tech*. Updated 13 November 2018. <https://ourdataourselves.tacticaltech.org/posts/whatsapp>
- Ricaurte, P. (2019). Data epistemologies, the coloniality of power, and resistance. *Television & New Media*, 20(4), 350–365. <https://doi.org/10.1177/1527476419831640>
- Richards, N. (2022). *Why Privacy Matters*. Oxford University Press.
- Richards, N. M. and Hartzog, W. (2020). A relational turn for data protection? 4 *European Data Protection Law Review* 1. <https://ssrn.com/abstract=3745973>
- Rohit, S. (2025, 15 April). Meta using WhatsApp and llama AI to power e-governance in India. *Medianama*. <https://www.medianama.com/2025/04/223-meta-whatsapp-llama-ai-e-governance-india/>
- Roy, A. (2021). This is no ordinary spying: Our most intimate selves are now exposed. *The Guardian*. <https://www.theguardian.com/commentisfree/2021/jul/27/spying-pegasus-project-states-arundhati-roy>
- Saffer, D. (2005). *The Role of Metaphor in Interaction Design*. Carnegie Mellon University.
- Saldanha, A., Rajput, P. and Hazare, J. (2018, 9 July). Child-lifting rumours: 33 killed in 69 mob attacks since Jan 2017. Before that only 1 attack in 2012. *IndiaSpend*. <https://www.indiaspend.com/child-lifting-rumours-33-killed-in-69-mob-attacks-since-jan-2017-before-that-only-1-attack-in-2012-2012>

- Sambasivan, N., Checkley, G., Batool, A., Ahmed, N., Nemer, D., Sanely Gaytán-Lugo, L. et al (2018). Proceedings of the Fourteenth USENIX Conference on Usable Privacy and Security (SOUPS '18). USENIX Association, USA, 127–142.
- Santos, M. and Faure, A. (2018). Affordance is power: Contradictions between communicational and technical dimensions of WhatsApp's end-to-end encryption. *Social Media + Society*, 4(3), 1–16. <https://doi.org/10.1177/2056305118795876>
- Sarasvati, N. (2024, 20 March). Rajya Sabha MP Saket Gokhale writes to IT ministry seeking information on Viksit Sampark WhatsApp message. *Medianama*. <https://www.medianama.com/2024/03/223-saket-gokhale-it-ministry-viksiti-bharat-sampark/>
- Sardar, Z. (1993). Colonizing the future: The 'other' dimension of futures studies. *Futures*, 179–187.
- Sarkar, T. (2001). *Hindu Wife, Hindu Nation: Community, Religion, and Cultural Nationalism*. Permanent Black.
- Schroeder, R. (2018). *Social Theory after the Internet: Media, Technology, and Globalization*. UCL Press.
- SCO. (2017a, 17 July). *Day 1 Arguments: Whatsapp-Facebook Privacy*. Supreme Court Observer. <https://www.scobserver.in/reports/whatsapp-facebook-privacy-karmanya-singh-sareen-day-1-arguments/>
- SCO. (2017b, 6 September). *Day 2 Arguments: WhatsApp-Facebook Privacy*. <https://www.scobserver.in/reports/whatsapp-facebook-privacy-karmanya-singh-sareen-day-2-arguments/>
- SCO. (2017c). *Fundamental Right to Privacy: Justice K.S. Puttaswamy v Union of India*. <https://www.scobserver.in/cases/puttaswamy-v-union-of-india-fundamental-right-to-privacy-case-background/>
- SCO. (2018, 26 September). *Constitutionality of Aadhaar Act: Judgment Summary*. <https://www.scobserver.in/reports/constitutionality-of-aadhaar-justice-k-s-puttaswamy-union-of-india-judgment-in-plain-english/>
- SCO. (2021, 15 February). *Day 3 Arguments: WhatsApp-Facebook Privacy*. Supreme Court Observer. <https://www.scobserver.in/reports/karmanya-singh-sareen-whatsapp-facebook-privacy-union-india-day-3-arguments/>
- Sethi, N. (2017, 4 May). Twitter @nit_set. https://x.com/nit_set/status/860018003596910592
- Shah, N. (2016). Free Basics by Facebook – An interview with Nishant Shah [Interview]. <https://spheres-journal.org/contribution/free-basics-by-facebook-an-interview-with-nishant-shah/>
- Shaikh, S. (2025, 21 September). From 'good morning' to AI: How WhatsApp is becoming the gateway to a billion Indians. *Livemint*. <https://www.livemint.com/ai/india-ai-adoption-through-whatsapp-11758449278183.html>
- Sharma, A. D. (2024). *The Backstage of Democracy: India's Election Campaign and the People who Manage Them*. Cambridge University Press.

- Sharma, M. (2022, 3 July). India's internet shutdowns: Looking beyond J&K, Rajasthan the new hotbed. *India Today*. <https://www.indiatoday.in/india/story/india-internet-shutdowns-looking-beyond-j-k-rajasthan-new-hotbed-1969664-2022-07-03>
- Sharp, J. (2011). Subaltern geopolitics: Introduction. *Geoforum*, 42(3), 271–273. <https://doi.org/https://doi.org/10.1016/j.geoforum.2011.04.006>
- Sharp, J. (2021). Materials, forensics and feminist geopolitics. *Progress in Human Geography*, 45(5), 990–1002. <https://doi.org/10.1177/0309132520905653>
- Sheikh, S. (2024). *How Technology Is (and Isn't) Transforming Election Campaigns in India*. Doctoral Dissertation, Yale University.
- Shipp, L. (2022). *Leaky Bodies, Leaking Data: Period Tracking Apps, Menstrual Capitalism and the Praxis of Feminist Cyber Security*. Doctoral Dissertation. Royal Holloway, University of London.
- Signal. (2016). Grand jury subpoena for Signal user data, Eastern District of Virginia. <https://signal.org/bigbrother/eastern-virginia-grand-jury/>
- Silverstone, R. (1994). *Television and Everyday Life*. Routledge.
- Silverstone, R. (2006). Domesticating domestication: Reflections on the life of a concept. In T. Berker, M. Hartmann, Y. Punie and K. J. Ward (Eds) *Domestication of Media and Technology* (pp 229–248). Open University.
- Singh, M. (2020, 26 April). Reliance and Facebook pilot JioMart grocery shopping on WhatsApp. *Techcrunch*. <https://techcrunch.com/2020/04/26/reliance-and-facebook-pilot-jiomart-orders-on-whatsapp/>
- Singh, M. (2021). India asks WhatsApp to withdraw new privacy policy over 'grave concerns'. *Techcrunch.com*. <https://techcrunch.com/2021/01/19/india-asks-whatsapp-to-withdraw-new-privacy-policy-expresses-grave-concerns/>
- Singh, N. (2024, 21 January). Ram mandir consecration: Timeline of dispute, judgement and key moments. *Business Standard*. https://www.business-standard.com/india-news/ram-mandir-consecration-timeline-of-dispute-judgement-and-key-moments-124012100188_1.html
- Singh, S. (2018a, 30 October). Fighting fake information is a societal challenge: Chris Daniels, WhatsAppE. *Economic Times*. <https://economictimes.indiatimes.com/tech/internet/fighting-fake-information-is-a-societal-challenge-chris-daniels-whatsapp/articleshow/66423678.cms?from=mdr>
- Singh, S. (2018b, 30 October). Want to keep WhatsApp the way it was built to be: Chris Daniels, Global head. *Economic Times*. https://economictimes.indiatimes.com/tech/internet/want-to-keep-whatsapp-the-way-it-was-built-to-be-chris-daniels-global-head/articleshow/66423834.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst
- Singh, S. S. (2019). *How to Win an Indian Election: What Political Parties Don't Want You to Know*. Penguin.

- Singh, T. (2021). Big opportunity! CCI accepts IFF's expert information in its investigation of WhatsApp's 2021 Privacy Policy. Internet Freedom Foundation. <https://internetfreedom.in/big-opportunity-cci-accepts-iffs-expert-information/?ref=static.internetfreedom.in>
- Singh, T. (2023). Supreme Court directs WhatsApp to allow users to continue using WhatsApp without accepting its 2021 Privacy Policy. Internet Freedom Foundation. <https://internetfreedom.in/supreme-court-directs-whatsapp-to-allow-users-to-continue-using-whatsapp-without-accepting-its-2021-privacy-policy/>
- Sinha, S. (2017). Fragile hegemony: Modi, social media, and competitive electoral populism in India. *International Journal of Communication*, 11, 4158–4180.
- Slay, J. (2016, 5 March). Why is Brazil trying to block WhatsApp? *The Conversation*. <https://theconversation.com/why-is-brazil-trying-to-block-whatsapp-58855>
- Solove, D. J. (2002). Conceptualizing privacy. *California Law Review*, 90, 1087–1155.
- Solove, D. J. (2013). Introduction: Privacy self-management and the consent dilemma. *Harvard Law Review*, 126(7). <https://harvardlawreview.org/print/vol-126/introduction-privacy-self-management-and-the-consent-dilemma/>
- Sonkar, S. (2022). *What Privacy Means: Why It Matters and How We Can Protect It*. Hachette.
- Spagnuolo, S. and Martins, L. (2022, 4 July). With zero-rating, Meta prevented open internet from emerging around the world, says Frances Haugen. *Núcleo Jornalismo*. <https://nucleo.jor.br/english/2022-07-04-zero-rating-meta-prevented-open-internet/>
- Spandana, R. S. and D'Souza, J. (2023). SCO daily: Is WhatsApp violating the right to privacy? *Supreme Court Observer*. <https://www.scoobserver.in/journal/sco-daily-is-whatsapp-violating-the-right-to-privacy/>
- Srikrishna, B. N. (2018). A free and fair digital economy: Protecting privacy, empowering Indians. Government of India. https://www.meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf
- Srivastava, M. (2023, 31 March). India hunts for spyware that rivals controversial Pegasus system. *The Financial Times*. <https://www.ft.com/content/7674d7b7-8b9b-4c15-9047-a6a495c6b9c9>
- Srivastava, S. (2015). *Entangled Urbanism: Slum, Gated Community and Shopping Mall in Delhi and Gurgaon*. Oxford University Press.
- Srivastava, S. (2021). Algorithmic governance and the international politics of big tech. *Perspectives on Politics*, 21(3), 989–1000. <https://doi.org/10.1017/S1537592721003145>
- Srivastava, S. (2023). Algorithmic governance and the international politics of big tech. *Perspectives on Politics*, 21(3), 989–1000. <https://doi.org/10.1017/S1537592721003145>

- Star, S. L. (1991). Power, technology and the phenomenology of conventions. In J. Law (Ed), *A Sociology of Monsters*. Basil Blackwell.
- Sudhir, K. and Sunder, S. (2020, 27 March). What happens when a billion identities are digitized? *Yale Insights*. <https://insights.som.yale.edu/insights/what-happens-when-billion-identities-are-digitized>
- Sukumar, A. M. (2019). *Midnight's Machines: A Political History of Technology in India*. Penguin Random House India.
- Suri, A. (2022). *The Great Tech Game*. Harper Collins.
- Talabi, K. (2022). Tailored to fit? WhatsApp Marketing in Nigeria's fashion industry. In I. Hassan and J. Hitchens (Eds) *WhatsApp and Everyday Life in West Africa: Beyond Fake News* (pp 73–86). Bloomsbury.
- Taraporevala, P. (2024, 24–25 June). *Who Needs Privacy? The (Un)making of Digital Personal Data Protection in India*. Workshop on Legal Geographies of the Digital Commons, Birkbeck, University of London.
- Tawa Lama-Rewal, S. (2007). Neighborhood associations and local democracy: Delhi municipal elections 2007. *Economic and Political Weekly*, 42(47), 51–60.
- Tech Desk. (2018). On issue of traceability, WhatsApp says 'will not weaken privacy protection'. *Indian Express*. <https://indianexpress.com/article/technology/social/whatsapp-on-traceability-will-not-weaken-the-privacy-protection-we-provide-5321576/>
- Tech, I.T. (2018). WhatsApp is finally and officially available on JioPhone and JioPhone 2, rollout starts. *India Today*. <https://www.indiatoday.in/technology/news/story/whatsapp-is-finally-and-officially-available-on-jio-phone-one-and-jio-phone-2-rollout-starts-1337328-2018-09-11>
- TechCrunch. (2014, 16 February). Facebook launches zero, a text-only mobile site for carriers. *TechCrunch*. <https://techcrunch.com/2010/02/16/facebook-launches-zero-a-text-only-mobile-site-for-carriers/>
- TechDesk. (2023, 4 March). Facebook CEO Mark Zuckerberg shares photos from Anant Ambani pre-wedding celebrations, says I love Indian weddings. *The Times of India*. <https://timesofindia.indiatimes.com/gadgets-news/facebook-ceo-mark-zuckerberg-shares-photos-from-anant-ambani-pre-wedding-celebrations-says-i-love-indian-weddings/photostory/108176488.cms?picid=108176579>
- Terranova, T. (2012). Attention, economy and the brain. *Culture Machine*, 13. <https://culturemachine.net/wp-content/uploads/2019/01/465-973-1-PB.pdf>
- Thatcher, J., O'Sullivan, D. and Mahmoudi, D. (2016). Data colonialism through accumulation by dispossession: New metaphors for daily data. *Environment and Planning D: Society and Space*, 34(6), 990–1006. <https://doi.org/10.1177/0263775816633195>

- Thaver, M. and Modak, S. (2021, 18 October). In Rhea Chakraborty, Aryan Khan arrests, NCB relies only on WhatsApp chats. *Indian Express*. <https://indianexpress.com/article/cities/mumbai/narcotics-control-bureau-aryan-khan-rhea-chakraborty-drug-case-whatsapp-chats-7577006/#>
- The Joe Rogan Experience. (2025). Mark Zuckerberg. [Video] YouTube. <https://www.youtube.com/watch?v=7k1ehaE0bdU>
- The New York Times. (2022, 31 January). The battle for the world's most powerful cyberweapon. *The New York Times Magazine*. <https://www.nytimes.com/2022/01/28/magazine/nso-group-israel-spyware.html>
- The Wire Staff. (2021, 4 August). Pegasus Project: 174 individuals revealed by the wire on snoop list so far. *The Wire*. <https://thewire.in/rights/project-pegasus-list-of-names-uncovered-spyware-surveillance>
- The Wire Staff. (2024, 1 March). US court orders NSO Group to handover code for spyware, Pegasus to WhatsApp. *The Wire*. <https://thewire.in/world/us-court-orders-nso-group-to-handover-code-for-spyware-pegasus-to-whatsapp>
- Thompson, C. (2019). *Coders: Who They Are, What They Think and How They Are Changing Our World*. Picador.
- Tilley, H. (2011). *Africa as a Living Laboratory: Empire, Development, and the Problem of Scientific Knowledge, 1870–1950*. University of Chicago Press.
- Times of India. (2024). WhatsApp Scams: Government gets 'alarm call' from India's Telecom Regulator. <https://timesofindia.indiatimes.com/technology/tech-news/government-sends-notice-to-whatsapp-after-scam-alarm-from-telecom-regulator-trai/articleshow/116020712.cms>
- TimesofIndia.com. (2021, 15 February). Supreme Court issues notice to centre, WhatsApp over new privacy policy. *The Times of India*. <https://timesofindia.indiatimes.com/business/india-business/supreme-court-issues-notice-to-facebook-whatsapp-over-new-privacy-policy/articleshow/80920037.cms>
- TimesofIndia.com. (2025, 22 August). Tamil Nadu launches WhatsApp-based chatbot offering easy access to government services. <https://timesofindia.indiatimes.com/technology/tech-news/tamil-nadu-launches-whatsapp-based-chatbot-offering-easy-access-to-government-services/articleshow/123450538.cms>
- Treré, E. (2020). The banality of WhatsApp: On the everyday politics of backstage activism in Mexico and Spain. *First Monday*, 25(1).
- Turow, J., Michael, H. and Draper, N. (2018). Persistent misperceptions: Americans' misplaced confidence in privacy policies, 2003–2015. *Journal of Broadcasting & Electronic Media*, 62(3), 461–478. <https://doi.org/10.1080/08838151.2018.1451867>
- Udupa, S. (2014). Aam Aadmi: Decoding the media logics. *Economic & Political Weekly*, 49(7), 13–15.

- Udupa, S., Gagliardone, I. and Hervik, P. (2021). *Digital Hate: The Global Conjunction of Extreme Speech*. Indiana University Press.
- Udupa, S. and Pohjonen, M. (2019). Extreme Speech | extreme speech and global digital cultures – Introduction. *International Journal of Communication*, 13(2019), 3049–3067. <https://ijoc.org/index.php/ijoc/article/view/9102>
- Udupa, S. and Wasserman, H. (2025). *WhatsApp in the World: Disinformation, Encryption and Extreme Speech*. New York University Press.
- UN. (1948, 10 December). Resolution 217A (III). UN General Assembly, Universal Declaration of Human Rights, A/RES/217(III),
- Vaidhyanathan, S. (2012). *The Googlization of Everything (And Why We Should Worry)*. University of California Press.
- Vaidhyanathan, S. (2018). *Anti-Social Media: How Facebook Disconnects Us and Undermines Democracy*. Oxford University Press.
- Valenzuela, S., Bachmann, I. and Bargsted, M. (2021). The personal is the political? What do WhatsApp users share and how it matters for news knowledge, polarization and participation in Chile. *Digital Journalism*, 9(2), 155–175.
- Valverde, M. (2014). ‘Time thickens, takes on flesh’: Spatiotemporal Dynamics in Law. In I. Braverman, N. Blomley, D. Delaney and A. Kedar (Eds) *The Expanding Spaces of Law: A Timely Legal Geography* (pp 53–76). Stanford University Press. <https://doi.org/10.1515/9780804791878-005>
- Varoufakis, Y. (2024). *Technofeudalism: What Killed Capitalism*. Penguin.
- Vega, N. (2021, 15 January). WhatsApp delays rollout of new privacy policy after backlash. *New York Post*. <https://nypost.com/2021/01/15/whatsapp-delays-rollout-of-new-privacy-policy-after-backlash/>
- Véliz, C. (2021). *Privacy is Power: Why and How You Should Take Back Control of Your Data*. Penguin.
- Venkatraman, S. (2017). *Social Media in South India*. UCL Press. <https://doi.org/10.14324/111.9781911307914>
- Viljoen, S. (2021). A relational theory of data governance. *The Yale Law Journal*, 131(2), 370–781.
- Vincent, J. (2016). Facebook’s Free Basics service has been banned in India. *The Verge*. <https://www.theverge.com/2016/2/8/10913398/free-basics-india-regulator-ruling>
- Vinsel, L. and Russell, A. L. (2020). *The Innovation Delusion: How Our Obsession with the New Has Disrupted the Work That Matters Most*. Currency.
- Vora, A. (2022). Find your central product metaphor. The hard parts of growth. https://amivora.substack.com/p/find-your-central-product-metaphor?utm_source=publication-search
- Vox Media Podcast Network. (2022). Land of the giants. *It’s a WhatsApp World*. <https://podcasts.apple.com/ph/podcast/its-a-whatsapp-world/id1465767420?i=1000577184486>

- Waghmare, A. (2024). Access to phones and the internet. *Data for India*. 29 February 2024. <https://www.dataforindia.com/comm-tech/>
- Wajcman, J. (2004). *Technofeminism*. Polity.
- Waldman, A. (2021). *Industry Unbound: The Inside Story of Privacy, Data, and Corporate Power*. Cambridge University Press. <https://doi.org/10.1017/9781108591386>
- Waldman, A. E. (2018). *Privacy as Trust: Information Privacy for an Information Age*. Cambridge University Press.
- Weinberg, L. (2017). Rethinking privacy: A feminist approach to privacy rights after Snowden and culture. *Westminster Papers in Communication and Culture*, 12(3), 5–20. <https://doi.org/10.16997/wpcc.258>
- West, S. M. (2019). Data capitalism: Redefining the logics of surveillance and privacy. *Business & Society*, 58(1), 20–41. <https://doi.org/10.1177/0007650317718185>
- WhatsApp. (2009). Just wanted to say a few things ... *WhatsApp Blog*. <https://blog.whatsapp.com/just-wanted-to-say-a-few-things?lang=uk>
- WhatsApp. (2010, 12 February). WhatsApp homepage. *Internet Archive Wayback Machine*. <https://web.archive.org/web/20100212212234/http://www.whatsapp.com>
- WhatsApp. (2011, 5 March). WhatsApp homepage. *Internet Archive Wayback Machine*. <https://web.archive.org/web/20110303184906/http://www.whatsapp.com/>
- WhatsApp. (2012a, 7 July). *Privacy Notice*. <https://www.whatsapp.com/legal/privacy-policy/revisions/20120707#:~:text=WhatsApp%20does%20not%20collect%20names,his%2Fher%20mobile%20address%20book>
- WhatsApp. (2012b, 18 June). Why we don't sell ads. *WhatsApp Blog*. <https://blog.whatsapp.com/why-we-don-t-sell-ads>
- WhatsApp. (2014a, 22 April). 500,000,000. *WhatsApp Blog*. <https://blog.whatsapp.com/500-000-000>
- WhatsApp. (2014b, 17 March). I would like to clarify. *WhatsApp Blog*. <https://blog.whatsapp.com/setting-the-record-straight>
- WhatsApp. (2016a, 5 April). end-to-end encryption. *WhatsApp Blog*. <https://blog.whatsapp.com/end-to-end-encryption>
- WhatsApp. (2016b, 25 August). Looking ahead for WhatsApp. *WhatsApp Blog*. <https://blog.whatsapp.com/looking-ahead-for-whats-app?ref=static.internetfreedom.in>
- WhatsApp. (2016c, 25 August). WhatsApp privacy policy. <https://www.whatsapp.com/legal/privacy-policy/revisions/20160825>
- WhatsApp. (2018a, 10 July). Labeling forwarded messages. *WhatsApp Blog*. <https://blog.whatsapp.com/labeling-forwarded-messages>
- WhatsApp. (2018b). More changes to forwarding. *WhatsApp Blog*. https://blog.whatsapp.com/more-changes-to-forwarding/?page_source=search&q=forwards

- WhatsApp. (2018c). WhatsApp privacy policy. *WhatsApp Blog*. <https://www.whatsapp.com/legal/privacy-policy-eea/revisions/20180424>
- WhatsApp. (2019, 19 December). 400 million stories. *WhatsApp Blog*. <https://blog.whatsapp.com/400-million-stories>
- WhatsApp. (2021a, May 2024). Answering your questions about WhatsApp's January 2021 Privacy Policy update. <https://faq.whatsapp.com/595724415641642>
- WhatsApp. (2021b, 15 January). Giving more time for our recent update. *WhatsApp Blog*. <https://blog.whatsapp.com/giving-more-time-for-our-recent-update>
- WhatsApp. (2021c). WhatsApp privacy policy. *WhatsApp Blog*. <https://www.whatsapp.com/legal/privacy-policy>
- WhatsApp. (2023). Private messaging showcase at Gateway of India in Mumbai. YouTube.com. https://www.youtube.com/watch?v=vprXR_OF2UI
- WhatsApp. (2024a, 16 February). Privacy policy. *WhatsApp Blog*. <https://www.whatsapp.com/legal/privacy-policy-eea#privacy-policy-information-we-collect>
- WhatsApp. (2024b). Welcome to the WhatsApp Business summit. *WhatsApp Blog*. <https://business.whatsapp.com/resources/resource-library/whatsapp-business-summit-india-24>
- WhatsApp. (2024c). WhatsApp Business messaging policy. *WhatsApp Blog*. <https://business.whatsapp.com/policy#:~:text=We%20prohibit%20the%20use%20of%20the%20WhatsApp%20Business%20Platform%20by,National%20Security%20and%20Intelligence%20Agencies>
- WhatsApp. (2025a). About end-to-end encryption. *WhatsApp Blog*. <https://faq.whatsapp.com/820124435853543>
- WhatsApp. (2025b). Ads that click to WhatsApp. *WhatsApp Blog*. <https://business.whatsapp.com/products/ads-that-click-to-whatsapp>
- WhatsApp. (2025c). Business platform pricing. *WhatsApp Blog*. <https://business.whatsapp.com/products/platform-pricing>
- WhatsApp. (2025d). Business platform, success stories. *WhatsApp Blog*. <https://business.whatsapp.com/resources/success-stories/dominos-pizza-indonesia>
- WhatsApp. (2025e). Business privacy. *WhatsApp Blog*. <https://business.whatsapp.com/privacy-protections>
- WhatsApp. (2025f). FAQs privacy and security for business messages. *WhatsApp Blog*. <https://faq.whatsapp.com/1148840052398648>
- WhatsApp. (2025g). Message privately. *WhatsApp Blog*. <https://www.whatsapp.com/privacy>
- WhatsApp. (2025h). Payments. *WhatsApp Blog*. <https://www.whatsapp.com/legal/payments/terms#:~:text=If%20you%20use%20Payments%2C%20you,our%20WhatsApp%20Payments%20Privacy%20Policy>

- WhatsApp LLC v Union of India* (Special Leave Petition), High Court of Delhi (2021).
- WhatsApp LLC v Competition of India & Anr*, High Court of New Delhi (2022).
- WhatsApp LLC v The Union of India*, Delhi High Court (2021).
- Wiener, A. (2020). Taking back our privacy. *New York Times*. <https://www.newyorker.com/magazine/2020/10/26/taking-back-our-privacy>
- Willems, W. (2019). ‘The politics of things’: Digital media, urban space, and the materiality of publics. *Media, Culture & Society*, 41(8), 1192–1209. <https://doi.org/10.1177/0163443719831594>
- Williams, P., Kamra, L., Johar, P., Khan, F. M., Kumar, M. and Oza, E. (2022). No room for dissent: domesticating WhatsApp, digital private spaces, and lived democracy in India. *Antipode*, 54(1), 305–330. <https://doi.org/https://doi.org/10.1111/anti.12779>
- Winner, L. (1988). *The Whale and the Reactor: A Search for Limits in an Age of High Technology*. University of Chicago Press.
- The Wire Wrap Episode 6: Electoral Bonds, Kejriwal’s Arrest, BJP’s MCC Violation*. (2024). https://www.youtube.com/watch?v=-lKUmc49pNI&ab_channel=TheWire
- Wired. (2018, 12 December). How WhatsApp fuels fake news and violence in India. <https://www.wired.com/story/how-whatsapp-fuels-fake-news-and-violence-in-india/>
- Woodyer, T. and Carter, S. (2020). Domesticating the geopolitical: Rethinking popular geopolitics through play. *Geopolitics*, 25(5), 1050–1074. <https://doi.org/10.1080/14650045.2018.1527769>
- World Economic Forum. (2011). Personal Data: The emergence of a new asset class. Opportunities for the telecommunications industry. https://media.bain.com/Images/WEF_Personal_Data%20A_New_Asset_Classes_Telecom_opportunities.pdf
- Wu, T. (2016). *The Attention Merchants: The Epic Scramble to Get Inside Our Heads*. Alfred A. Knopf.
- Wynn-Williams, S. (2025). *Careless People: A Cautionary Tale of Power, Greed, and Lost Idealism*. Flatiron Books.
- Yadav, S. (2020, 21 July). Interview: Avinash Pant on making of WhatsApp’s first global brand campaign. *Social Samosa*. <https://www.socialsamosa.com/2020/07/interview-avinash-pant-facebook/>
- YouTube. (2014a). *The Johns Hopkins Foreign Affairs Symposium Presents: The Price of Privacy: Re-Evaluating the NSA*. [Video] John Hopkins University. <https://www.youtube.com/watch?v=kV2HDM86XgI>
- YouTube. (2014b). *Mark Zuckerberg at the Mobile World Congress 2014* [Full Video]. <https://www.youtube.com/watch?v=VHwkHZpXqWc>

- YouTube. (2022). *Mark Zuckerberg en la WhatsApp Business Summit*. https://www.youtube.com/watch?v=iWqFreTUQJQ&ab_channel=C%C3%A9sarDergarabedian
- Yusoff, K. (2024). *Geologic Life: Inhuman Intimacies and the Geophysics of Race*. Duke University Press.
- Zuboff, S. (2019). *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. Profile Books.
- Zuckerberg, M. (2014). WhatsApp. *Zuckerberg Transcripts*, 977. https://epublications.marquette.edu/zuckerberg_files_transcripts/977
- Zuckerberg, M. (2015a, 28 December). Free Basics protects net neutrality. *The Times of India*. <https://timesofindia.indiatimes.com/blogs/toi-edit-page/free-basics-protects-net-neutrality/>
- Zuckerberg, M. (2015b). Mark Zuckerberg's post. <https://www.facebook.com/zuck/posts/10102530374780451?pnref=story>

Index

A

Aadhaar biometric identity system 2, 180
 constitutional challenges to 52–53, 96
 and data colonialism 54
 JAM trinity initiative 187, 191
 Puttaswamy case and 52–53, 96
 Supreme Court ruling on 53, 191
 Aam Aadmi Party (AAP) 72–73, 76–77
 accountability, performance of 44
 activist coordination 65
 Acton, Brian 7–8, 22–23, 90–91, 93, 123
 aversion to advertising 7, 13–14, 16, 24, 91, 93, 125
 departure from Facebook 24, 93
 on end-to-end encryption 126–128
 EU commission and 91
 Signal co-founder 126, 141
 advertising 21, 22, 90–91, 93, 178, 180–181
 Click-to-WhatsApp ads 178–179
 founders' opposition to 7, 13–14, 16, 24, 91, 93, 125
 metadata and targeted ads 141–143
 WhatsApp introduction of 180
 affect and emotion 64
 affective appeals to nationalism 70–71, 174
 affective publics 36
 feeling of privacy 135–137, 174
 frictive intimacies 61, 71
 agency (user) 45–46, 150, 156, 170–172
 Agrawal, Aditi 120, 142, 143, 167
 AI (artificial intelligence) 82, 84, 85, 181–182, 197, 206–207
 Aiyar, Alladi Krishnswamy 52
 algorithmic governance, social ordering through 32–33
 Ambani, Mukesh 194
 Ambedkar, B. R. 51, 52
 Amnesty International 164–165
 Andhra Pradesh 13, 83
 anti-corruption movements 62
 Apple 132
 iCloud data protection withdrawal 33
 privacy-enhancing technology 41
 Arab Spring 36, 62

Arora, Neeraj 128

Arora, Payal 37–39, 45, 54, 150, 172

Arthashastra (Kautilya) 50

Ashlin, M. 117

Ata, Maha Ravi 108

attention economy 16, 20–21

B

Babri Masjid 72

Balkin, Jack 33

Ballakrishnen, S. S. 47, 50

Banaji, S. 74

Barnett, C. 37

BBDO India 135, 136

Berners-Lee, Tim 18

Bhalla, A. 48

Bharatiya Janata Party (BJP) 2, 28, 72–73, 76, 82–84

2014 national elections 67–68, 82–83

2019 national elections 9, 28, 69, 71

2024 national elections and Viksit Bharat message 190–191

cell phone pramukhs 69, 72

Hindu nationalism and 67–70, 85

IT cell and WhatsApp strategy 28, 67–70

Modi as cult personality 28, 68

Bhat, R. 74

Bhima Koregaon case 168

Bidar, Karnataka 27

Big Tech 3–4, 32–35, 37, 40–44

legal entrepreneurialism 34, 87–88, 104, 112

lobbying by 34

privacy narratives 39–42, 88

private authority of 13, 85, 88, 115

techno-feudalism and 4, 25

wealthier than nation states 32

Boeing 34

Boellstorff, Tom 36

boundary work 46, 150, 155

family WhatsApp groups 61, 70–71

neighbourhood groups 76–77

Bratton, Ben 4, 30–31

Brazil 8, 24, 45, 64, 93, 128

WhatsApp ban in 128–129

- WhatsApp Business in 183
- zero rating and 17–18
- Brignull, Harry 101
- C**
- Cambridge Analytica 1, 3, 24, 96, 157
- Carmi, E. 105
- Carter, S. 55
- caste 5, 38, 47–48, 50, 69, 167
- Cathcart, Will 115–117, 123, 131, 137, 165, 166, 178
 - on encryption and privacy 130–131, 137
 - on Pegasus attack 165–166
 - on privacy and trust competition 115
 - on US WhatsApp growth 207
- Cavoukian, Ann 124
- Chaitanya Rohilla v Union of India & Others* 103, 107, 110–111
- Chan, Priscilla 194
- Chandrachud, D. Y. 53
- child kidnapping rumours 26–27
- Chundru, A. 179
- citizen journalists 63
- Citizen Lab 164, 167
- Citizenship Act, India, protests against amendment 1–2
- Citizenship Amendment Act (CAA)
 - protests 1, 167, 172–173
- civil society 27, 54, 87, 96, 99, 117, 119, 164
 - activism against Free Basics 18–19
 - Internet Freedom Foundation 98, 100
 - privacy activism in India 87, 96–97
- code power 14
 - encryption as 131–132, 147
 - geopolitical dimensions 129–132
 - Santos and Faure on 127–129, 206
- Cohen, Julie 34, 42–44, 86, 88, 104–105, 112
- Cole, David 139
- colonialism 4, 6, 19, 35–36, 39, 51, 54
 - British colonial rule in India 47–48, 51, 146
 - data colonialism 4, 35–36, 39, 57, 147, 194, 202
 - digital colonialism 4, 19, 202
 - Indian Telegraph Act 1885 and 51
- commercial interests 41
- Competition Commission of India (CCI) 96, 112–113, 194
 - 2021 privacy policy investigation 99–100, 102–103
 - penalty imposed on Meta 100, 113
 - WhatsApp appeal against 100, 113
- computational totality 30–31
- consent (digital) 43–44, 100–106
 - dark pattern design and 101
 - feminist critique of 103–106
 - fiction of 103–106, 121
 - notice and consent model 43, 87, 112
 - trick consent 101
 - uncontracts 105
- Couldry, N. 35
- COVID-19 pandemic 12, 73–74, 99, 198
 - anti-Muslim messaging during 78–80
 - neighbourhood surveillance during 79–82
 - RWA WhatsApp groups and 79–82
 - WhatsApp political campaigning during 73
- D**
- Daniels, Chris 27, 130, 179, 194
- dark patterns 101
- data capitalism 14, 34, 96, 104, 144
 - extraction and profit 4, 35, 104
 - social quantification sector 40
- data colonialism 4, 35–36, 39, 57, 147, 194, 202
 - digital peripheries and 6, 37–39
 - WhatsApp and India 6, 54, 144
- data localization
 - DPDPA and 114
 - Indian government demands for 193–194
- data mining 13–14, 18
- Data Protection Bill 54, 113–114
- data protection legislation 54, 86–87, 94–96, 113–114
- Digital Personal Data Protection Act 2023 54, 87, 114, 191
- GDPR (EU) 2, 53, 86, 95, 111
- IT Act 2000/Amendment 2008 53–54, 95
- IT Rules 2021 84, 96, 118–120
- data relations 40
- data revolution 38
- data universalism 38, 40–41
- Datta, Bishakha 101, 106
- Daub, Adrian 57
- de Souza, P. S. 41
- decolonial approach to privacy 39
- democracy 5, 25, 85–86
 - digital private spaces and 2, 36–37, 60–65, 85
 - erosion, in India 60, 68
 - Hindu nationalism and 36, 60, 70–71
 - Papacharissi on digital 36–37, 61–63
 - private sphere and 36–37, 61–62
- Devanathan, Sandhya 145–146, 195–196, 206
- DigiLocker 13
- digital architectures 31, 46, 106, 122, 125, 163
- digital fiefdoms 35
- Digital India initiative 10, 19, 82–84, 195
- digital living room metaphor 3, 5, 46, 133–135, 174
 - feminist critique of 134
 - western/patriarchal construct 134, 206
 - Zuckerberg on 3, 133–134

digital peripheries 6, 37–39, 149, 205

digital populism 63

digital public infrastructure (DPI)

India Stack 83

WhatsApp and 83–84, 195

digital publics 12–13, 32, 36, 64–65

disinformation 25–26, 60, 64, 66–67, 72

BJP and 28, 67–70, 72

mob violence and 26, 72

WhatsApp University 12, 66

Divan, Shyam 113

Dixon, N. 79

domestication theory 5, 6, 32, 55–56, 132, 150, 158, 179

double articulation of technology 56

of end-to-end encryption 132–137, 158–164

feminist geopolitics and 55

Draper, N. 43

Dubey, D. K. 78

Durand, Cédric 4

Dzodan, Diego 128

E

Electronic Frontier Foundation 23

Elwood, S. 3, 149

emotional aspects of privacy *see* affect and emotion

encryption, end-to-end 1, 2–3, 23, 25–29, 65, 116, 122–125

as code power 129–132, 147, 206

as deflection from metadata 138–143, 147

domesticating 132–137, 158–164

geopolitics of 125–132

implementation by default (2016) 13–14, 23, 126–128

Indian government and traceability 27, 96, 118–120, 129–131

lived encryptions 5

Marlinspike, Moxie and 126

misunderstanding among users 158–164

as privacy thing 132, 147, 150, 158–163

Signal Protocol 126

user cynicism about 160–164

England, land enclosure movement in 35

Escobar, Arturo 125, 147

EU Commission 21, 89

European Union

Commission and Facebook acquisition 16, 89–91, 95

finances on Meta 34, 95

GDPR 2, 53, 86, 95, 111

F

Facebook 14–15, 20–22, 89–95

acquisition of WhatsApp 15–16, 89

Cambridge Analytica scandal 1, 3, 24, 96

data sharing with WhatsApp 22–23, 90–93

F8 Developer Conference (2019) 2–3

Free Basics/internet.org 17–19

privacy policy integration 22–23, 91–93

zero rating 17–18

see also Meta

fake news 26–27, 64, 66

family WhatsApp groups 174

extended family groups 69–71

good morning messages 12

political content in 59, 61, 69–71

Farrow, Ronan 164

Faure, A. 127, 128, 206

feminist geopolitics 4–5, 34, 37, 45, 55, 204

domesticating geopolitics 55–56

feminist technoscience 4, 30, 56, 123–124

intimate global 55, 71

planetary scale and 30–31

situated knowledge 31, 133

Foer, Franklin 57

forwarding messages 20, 26–27, 60, 66–70

five-chat limit imposed 27, 73

India as global leader in 27

political messaging and 68–70

Frampton, Kenneth 122

Free Basics/internet.org 17–19

Frew, S. 31

Fuchs, Christian 40–41

G

Gagliardone, I. 36

Gajda, A. 42

Gajjala, R. 48

gender and privacy 5, 38, 155–157

Lakshman Rekha allegory 50

patriarchal structures and 46–48, 50, 61

privacy work among women 46, 156, 170–172

purdah system 50

South Asian mobile phone sharing 48

surveillance of women 48–50, 80

geographies, of product 9

ghar and *bahir* (India) 48

see also public/private distinction

Gheorghe, Claudiu Dan 164

global south 6, 54, 183

digital peripheries 6, 37–39, 149, 205

as testbed/petri dish 9–10, 12, 196, 206

WhatsApp's initial growth markets 8–12

Gokhale, Saket 191

Google 32, 41, 44, 116

India freezing smartphones investigation 12

privacy policy 41

privacy-enhancing technology 41

governance, algorithmic 33

governance, digital 28, 195–196

WhatsApp and government services 12–13, 83–84

WhatsApp governance in Andhra Pradesh 13

Grosser, Ben 16–17
group chats 20, 79, 125, 169

H

Harsha Gupta v WhatsApp & Ors 102
hate speech 26
anti-Muslim content 59, 66, 69–70, 74–80
COVID-19 and 78–80
extreme speech 9, 36, 60, 66–67
Haugen, Frances 17–18
Haupt, J. 56–57
Hayden, Michael 139
Hervik, P. 36
Hindu nationalism/Hindutva 2, 5, 28, 36,
59–60, 82, 85
digital ecosystem for 67–70
neighbourhood groups and 74–79
Ram Mandir inauguration 71–72
subterranean storytelling infrastructure 60,
68, 70–72, 85
WhatsApp and rise of 60, 67, 85
Hoepman, Jaap-Henk 40, 125, 127, 139
Hoffman, A. L. 57

I

Igo, S. E. 3, 42
India 1–6, 37, 49–54
2014 general election 67–68, 82–83
2019 national elections 9, 28, 69, 71
2024 national elections 28, 190–191
biometric data *see* Aadhaar biometric
identity system
data sovereignty 109–111, 121
digital divide 10, 38
Digital India programme 10, 19, 82–84, 195
Jio/Reliance data packages 10, 19
national elections 8, 57, 68–69, 83,
190–191
National Optical Fibre Network 10
post-colonial privacy history 49–54
privacy as fundamental right 2, 53, 96, 157
Puttaswamy judgment 53–54, 95–96,
114, 119
voting rates in 62
WhatsApp and *see* WhatsApp entries
India Stack 52, 83, 193
Indian Constitution
Article 21 right to privacy 2, 53
Constituent Assembly debates 51–52
fundamental rights 51–53, 96
Indian government 1–2, 27–28, 53–54, 87
algorithmic governance 84
internet shutdowns 84–85
IT Intermediary Rules 2021 84, 96,
118–120
Pegasus spyware use allegations 165–167
traceability demands 27, 96, 118–120,
129–131

WhatsApp Business violation 190–192
WhatsApp litigation 96, 107–108, 114–121
Indian National Congress 62, 75, 192
Indian Telegraph Act (1885) 51
IndiaSpend data 26
inferred data 139
Information Technology (Amendment)
Act (2008) 53
informational capitalism 32, 34, 41–42,
86, 121
internet activism 19, 62
Internet Coalition 18
Internet Freedom Foundation (IFF) 98, 100
internet.org 16, 18
intimacy and trust 68, 70
intimate global 55, 71
IT Intermediary Rules 2021, WhatsApp
petition against 96, 118–120

J

Jain, Tripti 117
Jeffrey, Alex 112
JioMart 24, 183
JioPlatforms/Reliance Jio 10, 19, 24, 194
journalists and activists, and Pegasus
spyware 165

K

Kannabiran, K. 47, 50
Kantrowitz, Alex 116, 131
*Karmanya Singh Sareen v Union of India &
Ors* 97–99, 101, 109–114
Delhi High Court proceedings 97–98
European comparison argument 110–111
petition filed (2016) 97
Special Leave Petition 98, 110
still pending 99, 114
Karusala, N. 48
Kenya 65
Kitchin, R. 131
Koum, Jan 7–8, 20–21, 22–23
aversion to advertising 7, 13–14, 125
departure from Facebook 24
on encryption 126–128, 129
Ukraine background 14
Kumar, N. 48
Kumar, Rajendra 165
Kumar, Ravish 66
Kustomer 24

L

legal entrepreneurialism 6, 34, 88, 104,
112, 121
Leszczynski, A. 3, 149
literacy, privacy 172
lived encryptions 5
lobbying 18, 34, 114
Lockheed Martin 34

Lok Janshakti Party (LJP) 73

Low, M. 37

lynchings/mob violence 26–27, 70

M

MacKinnon, Catherine 46–47

Malaysia 65–66

Mandi, Himachal Pradesh 72

marital privacy, Indian Penal Code on 50–51

Marlinspike, Moxie 126, 141

Marques, Sandra 128

Marwick, Alice 37–38, 42–43, 45–46,
48–49, 150, 156–157, 170

Matthan, Rahul 51–52, 95

Mayer, J. 138

McDonald, T. 56

Mehta, Tushar 113

Mejias, U. A. 35

‘merely metadata,’ metadata as 144

Meta (previously Facebook) 3–4, 24–25,
32–34, 86–89

10-Q reports 86, 88, 94

earnings calls 16, 93, 182–183, 207

family of apps 3, 7, 14, 179

Llama AI 84

privacy pivot (2019) 2–3, 5, 133

private authority 13–14, 25, 85, 88,
115, 147

WhatsApp acquisition price 16

see also Facebook; WhatsApp

metadata 4, 22–23, 93

collection by WhatsApp 139–141

compared to content 138–139

encryption and deflection from
138–143, 147

General Hayden on killing with 139

NSA and 138–139

privacy implications 138–141, 163

Signal comparison 141–142

types (volunteered/observed/inferred) 139

metaphor

container metaphor 134, 145

digital living room 3, 5, 46, 133–135, 174

padlock metaphor 134, 145–146

tonic metaphor 5, 31–32, 56, 205

town square metaphor 3, 133

Mexico 65

Michael, H. 43

middle classes 38, 59, 61, 74–76, 79, 81, 153,
157, 167

minorities, religious and political 38, 59–61,
85, 175

exclusion from neighbourhood
groups 76–79

Muslim community (India) 1–2, 66–67,
69–70, 75–80, 155–157

privacy work by 155–157, 170–173

state surveillance of 1, 167–169

misinformation 5, 8, 59–60, 64, 66–67, 72

forwarding limits and 27

good morning messages and 12

mob violence and 26–27

WhatsApp Uncle archetype 12

WhatsApp University idiom 12, 66

Mitchell, J.C. 138

Modi, Narendra 2, 10, 28, 59, 67,
165–166, 206

Digital India flagship policy 82–83

Pegasus and Netanyahu meeting 165

Ram Mandir inauguration 71–72

Viksit Bharat Sampark WhatsApp
message 190–192

WhatsApp channel launch 84

Zuckerberg embrace (2015) 32

Mukerjee, Subhayan 18

Mukiri Smith, H. 41

Mutchler, P. 138

N

Nanda, A. S. 125

Narayan, S. S. 73

Narayanan, S. 73

National Register of Citizens (NRC) 167

neighbourhood WhatsApp groups 69

anti-Muslim content 76–79

authoritarianism and 75, 81–82

COVID-19 and surveillance 79–82

Resident Welfare Associations
(RWAs) 74–77

net neutrality 18–19

Netanyahu, Benjamin 165

network effect 5, 102, 115, 163–164, 176, 182

networked privacy 43

Nippert-Eng, Christena 46, 149–150

‘notice and consent’ model 43

NPCI, phased approval of WhatsApp
Pay 193

NSO Group/Pegasus spyware 118, 164–167

Indian government allegations 165–167

spyware mechanism 164

WhatsApp lawsuit against 118, 166

Nussbaum, Martha 47–48, 49

O

Obama, Barack 139

observed data 139

Olson, Parmy 8, 22, 91

Omanga, Duncan 64–65

Open Access protocols 34

Open Network for Digital Commerce
(ONDC) 195

Open Whisper Systems 126

P

Pant, Avinash 136

Papacharissi, Zizi 36–37, 61–63

- Pasad, Subramonium 108
 Pateman, Carole 47, 104
 Pegasus spyware 164–167
 planetary scale computation 4, 30–31, 32
 platform sovereignty 25
 political campaigns and WhatsApp 28,
 83–84, 190–193
 Aam Aadmi Party (AAP) 72–73
 backstage of democracy 28, 65, 68
 BJP 28, 66–74, 76, 82–85
 democracy and 59–66
 digital public-private infrastructures 82–85
 neighbourhood groups 74–82
 smaller parties 73
 WhatsApp Business prohibition
 on 190–192
 Pope, Richard 124
 privacy, definitions and concepts 3–4, 50–52,
 151–158
 decolonization of privacy studies 37–39
 feminist critique 4, 37–39, 46–47
 Indian equivalents and terms 49–50, 154
 as individual right 42, 105
 networked privacy 43
 relational approach to 38, 43
 as spatial practice 46–50, 151
 privacy architectures 13–15, 30–31, 204
 affective dimensions 13, 54–55
 discursive dimensions 13, 87–88
 legal dimensions 13, 86–88
 technical dimensions 13, 122, 124
 privacy frustration/cynicism 161, 173, 175
 privacy myths 5, 40, 144
 privacy policies (WhatsApp) 5, 86–91,
 120–121
 2012 privacy notice 90, 109
 2016 update 14, 22–23, 91–94, 97–99, 109
 2021 update 24, 93–94, 99–103, 115, 181
 anti-user practices 100–103
 backlash to 2021 update 25, 94, 96, 100,
 115–117
 European versus Indian users 94–95, 98,
 110–111
 Flesch-Kincaid readability 102
 geolegalities 106–114
 as performative 43, 87
 privacy game 115–120
 privacy policy fiction 103–106
 as socio-legal contract 6, 87, 103
 take-it-or-leave-it (2021) 24, 94, 99, 103
 privacy poor 45, 150
 privacy rich 45, 150
 privacy self-governance 44
 privacy techtonics (framework) 5–6, 29,
 30–32, 204–207
 digital private space as political 46–49
 as feminist geopolitics framework 30, 37
 post-colonial India, privacy in 49–54
 privacy and power 39–46
 reading privacy stories 57–58
 scalar approach 30
 sensing privacy 54–56
 situating privacy 37–39
 tectonic shifts 32–37
 tectonic analogy 5, 30
 tonic metaphor 5, 31–32, 56–57, 205
 privacy things 132, 147, 150, 158–163
 privacy work 2, 45–46, 156–157, 170–176
 among women 46, 156, 170–172
 boundary work and 46, 150
 informal hacks 162, 171–172, 175
 Marwick on 45, 150, 156, 170
 safety work 156
 unevenly distributed 45, 157, 175, 206
 privacy-by-design 14, 122–125,
 147–148, 205
 Cavoukian, Ann on 124
 code power 129–132
 commercial value of 125
 digital private lives, privatization
 of 143–147
 domesticating encryption 132–135
 feeling and performing privacy 135–138
 metadata and 138–143
 privacy as control illusion 146, 206
 privacy layers (WhatsApp) 144,
 180–181, 206
 see also encryption, end-to-end
 Proferes, N. 57
 ProPublica 9, 135, 182
 public trust, and Pegasus spyware 167
 public/private distinction 36–37, 46–48,
 60–61, 64–65
 Pulwama attacks 76–77
Puttaswamy v Union of India 95–96, 114, 119
 landmark 2017 judgment 2, 53–54,
 96, 157
 nine-judge bench 53
 WhatsApp lawsuit and 119
- R**
- Rau, Benegal Narsing 52
 Reliance (telecommunication company) 10
 Reliance Jio Platforms 24
 Resident Welfare Associations (RWAs) 74–77
 grassroots authoritarianism 74–75, 81–82
 Manor Park group 78, 81
 origins and structure 75
 surveillance practices 80–82
 Rest of the World 71–72
 Ricaurte, Paola 147
 Rich, Jessica 89
 Richards, Neil 40, 138, 146
 Rogan, Joe 34
 Rohatgi, Mukul 108
 Rohilla, Chaitanya 103, 107, 110–111

Rohini, G. 109

Roy, Arundhati 166

rumours 26–27

Russel, Andy 7

S

Sachdeva, Sanjeev 107

Saffer, D. 133

Salve, Harish 107, 113

Sambasivan, N. 48

Sandberg, Sheryl 22, 93, 127–128, 140

Santos, M. 127, 128, 206

Sardar, Ziaduddin 57

Sareen, Karmanya Singh *see Karmanya Singh
Sareen v Union of India & Ors*

Sarkar, Tanika 47

Scheiber 172

Sequoia Capital/Goetz, Jim 8

Sethi, Nitin 49, 53

Shah, Amit 69–70

Shah, Nishant 19

Sharp, Jo 55

Shaw, Robert 133

Shinde, Gauri 135

Shoshana, Zuboff 34, 104–105

Sibal, Kapil 113, 141

Signal 66, 117, 163, 175

Acton and Marlinspike co-founders 126, 141
minimal data collection 141–142

Silicon Valley 3–4, 6, 8, 13, 19, 22, 28,
32, 175

dominant culture of 124

future imaginaries 56–57

worldview 207

Singh, Karmanya 101

Singh, Shivam Shankar 28, 68

Snowden, Edward 96

Sonkar, S. 50

South Africa 79

South Asia 48

sovereignty, data/national 84, 107,
109–111, 121

Spain 65

spatial privacy 46

Srikrishna, B. N. 54, 114

Srinivas, Arun 196

Srivastava, Swati 32–33, 115

Suri, A. 115

surveillance 14, 164–170

Aadhaar and 52–54

of Muslim minority 1–2, 168–169

neighbourhood 80–82

Pegasus spyware 164–167

Soviet Ukraine legacy 14

state surveillance in India 1, 51–52,
167–170

surveillance capitalism 4, 32, 86, 104–105

surveillance capitalism 34

T

Tablighi Jamaat incident 79

Tamil Nadu 83

targeted advertising 25

taxonomy of personal data 139

Taylor, L. 41

techno-feudalism 4, 6, 25, 32

techno-optimism 56, 174, 175, 198, 203

Telegram 25, 66, 117, 128, 163, 175

Terranova, T. 20

Tharoor, Shashi 166

Thompson, Clive 123

traceability 27, 96, 117–120, 122, 129–131

TRAI ruling 18–19

Treré, E. 65

Trump, Donald 28, 32, 34

trust 8, 14, 21, 88, 155, 167, 198

competition for 115

as corporate currency 205

network effect and 67, 70

WhatsApp rebuilding after

backlash 115–117

Turow, J. 43

U

UAPA (Unlawful Activities Prevention
Act) 166, 168, 173

Udupa, S. 36

UK 33, 111

Unique Identification Authority of India
(UIDAI) 52, 95

UPI (Unified Payments Interface) 83, 193

urban middle classes 75

US 48–49, 150

clause about the data transfer to 109–110

content and metadata, distinction

between 138–139

Federal Trade Commission (FTC) 21,
89–90, 112

information processing industries 42

internet-based messaging market in 9–10

V

Vaidhyanathan, Siva 19, 44

Varoufakis, Yanis 35

Véliz, Carissa 39, 42

Venkataramkrishnan, Rohan 164–165

Venkatraman, Shriram 12

Vikasheel Insaan Party 73

Viksit Bharat Sampark message 190–192

Vinsel, Lee 7

volunteered data 139

Vora, Ami 135

W

Wajcman, J. 124

Waldman, Ari 13. 44, 87–88, 106, 131,
146, 205

- Weinberg, L. 104, 105
- West, S. M. 105
- WhatsApp 1–6
- 2009 founding 7–8
 - accessing official documents through 12–13
 - active daily users metric 21
 - attention economy and 19–21
 - brand campaigns in India 135–137, 144–146
 - campaign for 144–146
 - COVID-19 and 12, 73–74, 78–82
 - encrypted messages 3
 - forwarded messages labelling 27
 - forwarding limits 27
 - Gateway of India campaign 144–146
 - global users 7
 - good morning messages 12
 - India as largest market 10, 205
 - initial growth markets 9
 - interoperability 8
 - MAUs 12, 20–21
 - media campaign 135–137
 - mediating digital party-political intimacies 68
 - monetization of 16–17, 178–179
 - petition against IT Intermediary Rules 2021 96, 118–120
 - privacy architectures 13–15, 55
 - private authority, power of 13, 25
 - private enclosure ('digital ghar') 48
 - 'public power' of 107
 - as public utility 13, 107–108
 - revenue 25
 - role in political campaigning 63–64
 - simplicity design principle 8, 123, 125
 - targeted campaign messages 28
 - voice calling feature 10, 12
- WhatsApp Business 6, 23–24, 93
- beta testing for 24, 193
 - catalogue feature 178, 200
 - click-to-WhatsApp ads 178–179
 - erosion of privacy through 180–183, 202–203
 - Government of India and monetizing WhatsApp 193–194
 - India pilot (2018) 24, 179, 194
 - Modi's violation of policy 190–192
 - phone number as public object 186–190
 - platform versus app 177–178
 - small businesses and 196–202
 - for social and economic good 194–196
 - spam and user experience 177–178, 184–186
 - women entrepreneurs and 200
- WhatsApp governance 13
- WhatsApp groups 10, 20, 79, 125, 169
- see also* family WhatsApp groups
- WhatsApp LLC v Competition of India & Anr* 108
- WhatsApp Pay 24, 93, 193–194
- WhatsApp Uncle 12, 66
- WhatsApp University 12, 66
- WhatsApp v The Union of India* 118–119
- Woodyer, T. 55
- World Economic Forum 139
- Wu, Tim 20
- Wynn-Williams, Sarah 33
- X**
- X (formerly Twitter) 49, 50, 65, 84, 154
- Z**
- zero rating
- Brazil and 17–18
 - Facebook Zero 17–18
 - India prohibition of 18–19
- zero-click exploit, and Pegasus spyware 164
- Zimmer, M. 57
- Zuboff, Shoshana 32, 86, 104–105
- Zuckerberg, Mark 21–24, 140, 179, 204–207
- acquisition of WhatsApp 15–16
 - on digital living room 3, 133–134
 - Facebook future imaginaries 56–57
 - 'the future is private' declaration 2–3, 56, 149, 204
 - on growth obsession 16–17
 - on messaging as future 24
 - Modi embrace (2015) 32
 - on monetizing WhatsApp 16, 21–22
 - and WhatsApp's co-founders, rift between 24

