



BALANCE

CHALLENGING AND REIMAGINING DIGITAL POWER

ISSUE 01/2025

**DESIGNED FOR CONTROL:
Infrastructure, Power and
the Public**

**GROWING SIDeways:
The Seapunk Imagination**

Plus:

Who Writes the Rules?

App Store Censorship

Navigating The Labyrinth

Campaigns, Clicks, and Complicity

Australia's Tech Regulation Landscape

**and more Features, Perspectives and
Interviews inside...**

Welcome to the first issue of **BALANCE** Magazine

Thank you for opening up this first issue of *BALANCE*. It's the publication for a community of readers, writers, and makers who are thinking deeply about digital power—how it shapes the world we live in, and how resistance, care and imagination might help shape it differently.

Today, digital systems influence how we live, connect, move, work, and dream. They monitor our behaviour, steer economies, and redraw the political and planetary landscape. Power has consolidated. Surveillance has scaled. The early promise of the digital has been repackaged, monetised, and militarised.

Designed for speed, scale, and control, these systems often serve dominant interests. But beyond the mainstream, other paths are taking root—systems grounded in community, justice, and life. These alternatives grow slowly and quietly, at the speed of trust.

BALANCE is a space for critique and imagination. A place to examine how power operates, to trace its effects, and to notice what else is emerging. It explores the evolving relationship between technology, people, politics, and the planet—and invites you to ask: what's unfolding, what's possible, and what futures might we build together?

This magazine is aiming to be published at least three times a year. Its rhythm reflects the conditions of the moment. The Balance platform, our online presence, will be continuously updated with news and views.

We welcome your engagement with Balance, and look forward to your readership and support

Support the **BALANCE** Fund
Your support helps us
keep this space alive.



Subscribe from Now and 2026
Be part of what comes next.



Why *Balance* Exists

I was at university when I first used a web browser. It was an exciting time when the internet felt full of possibilities and the dot-com boom was just beginning. *Wired* magazine burst onto the scene in 1993, calling itself the chronicle of the emerging Digital Generation, “the most powerful people on the planet today.” Its editor, Louis Rossetto, opened that first issue with a vivid metaphor: “The Digital Revolution is whipping through our lives like a Bengali typhoon.”

Rossetto was referring to the Bhola Cyclone, one of the deadliest storms in history, which struck what is now Bangladesh and killed hundreds of thousands of people. He later acknowledged regret over using the metaphor, but it was still a telling choice — an image of such destruction used to celebrate speed, force, and inevitability. A couple of decades later, Silicon Valley echoed that same uncritical embrace of disruption, such as mottos like Facebook’s “move fast and break things” that rarely considered the human or social cost.

Over the last fifteen years, I have worked with people and organisations in journalism, human rights, and digital rights. In the earlier part of this period, technology and platforms like the then-Twitter, Facebook and Whatsapp, played a vital role in helping activists and communities get messages out, especially in the face of state censorship. These platforms still continue to be a space for freedom of expression, but they can also act as gatekeepers. They featured the ability to algorithmically block, downgrade, or distort visibility, often without transparency or accountability.

Technology is deeply embedded in almost every aspect of life, and its governing structures are more centralised, complex, and entrenched than ever. The same systems that once promised openness are now difficult to critique, challenge and make less harmful. The digital rights communities, tech policy specialists and tech justice activists are doing important work, yet this work often happens in silos and is sometimes influenced by funding agendas. This fragmentation often makes it harder to respond to the scale and complexity of the challenges we face.

We now live in a world shaped by a digital power bloc, a global concentration of corporate platforms, state systems, and infrastructure that shapes politics, economics, culture, and the environment. This bloc does not just build tools or set rules. It captures and isolates us, and subtly rewires how we relate to each other and to the world. There is a growing resistance movement to this bloc and *Balance* exists to connect the silos, and document this movement.

Balance is a platform and publication for sharing stories that explore, challenge, and reimagine digital power across borders and disciplines. It is a space for sharing knowledge and ideas, tracing how digital systems shape our world and imagining better digital futures. *Balance* brings together strategies, stories, and creative thinking that can push back against the bloc and help reclaim digital power for the public good.

Balance is produced in a lean way by a small team of committed people. Thank you to Pamodi, Kirsten and Indika for their hard work, and to everyone whose contributions made this first issue possible. I hope you find it useful, thought-provoking, and inspiring.

— Sam de Silva (September 2025)

Credits

PRODUCER / LEAD

Sam de Silva

EDITOR

Kirsten Han

<https://kirstenhan.com>

EDITORIAL ASSOCIATE

Pamodi Hewawaravita

DESIGN/LAYOUT

Indika Sriyan Gammudali

CURATORIAL TEAM

Sam de Silva, Pamodi
Hewawaravita and Archit Lohani

CONTRIBUTORS:

Aishik Saha

Benjamin Ismail

Katherine Francisco

Kirsten Han

Lizzie O'Shea

Miraj Chowdhury

Pamodi Hewawaravita

Patrick Boehler

Pradipa P. Rasidi

Prarthana Mitra

Ranjitha Kumar

Vinay Narayan

Saritha Irugalbandara

PRINTER

GB Gerakbudaya Enterprise Sdn. Bhd.

<https://www.gerakbudaya.com/>

PUBLISHER AND CONTACT

Common Edge Asia

balance@commonedge.asia

ISSN: 3083-5232

DIGITAL VERSION



COPYRIGHT AND LICENSE

© 2025 Balance and respective contributors. Some rights reserved. Content is published under a Creative Commons Attribution-NonCommercial 4.0 International License (CC BY-NC 4.0). Non-commercial use with attribution is encouraged.

DISCLAIMER

Balance is an independent publication featuring diverse views and creative works. Opinions are those of the contributors and do not necessarily reflect those of the editors or publishers. While accuracy is a priority, Balance is not liable for errors or reliance on this material. Content is informational only and not legal, financial, or professional advice.

Contents

COVER STORIES

Designed for Control: Infrastructure, power and the public

by Pamodi Hewawaravita

Page 04

Growing Sideways: The Seapunk imagination

a conversation with Sam Chua

Page 58

FEATURES

Who Writes the Rules? The new order of platform power

by Miraj Chowdhury

Page 09

A Just Transition to an AI Future: Pursuing a labour-first AI agenda

by Ranjitha Kumar and Vinay Narayan

Page 18

Power Plays: The uncomfortable position between governments and tech companies

by Saritha Irugalbandara

Page 37

Platform Power and Populism: The architecture behind Hindu nationalism's digital rise

by Aishik Saha

Page 44

PERSPECTIVES**Navigating the Labyrinth: Finding community on social media**

by Katherine Francisco

Page 22

"Show Us Your Screens": Algorave and the radical joy of live coding

by Prarthana Mitra

Page 12

Resisting Oppression: Focusing on information needs

by Patrick Boehler

Page 26

Documenting Resistance, Building Alternatives: The App Censorship Project and the struggle for digital freedom in Asia

by Benjamin Ismail

Page 48

DISPATCHES**Networks and Minefields: When social media presents both opportunity and risk**

by Kirsten Han

Page 30

False Starts and Stalled Reforms: Australia's tech regulation landscape

by Lizzie O'Shea

Page 34

Campaigns, Clicks and Complicity: How civil society actors built the 'buzzer' industry

by Pradipa P. Rasidi

Page 53

INTERVIEW**From Recruitment to Resistance**

a conversation with Aizat Shamsuddin

Page 41

Designed for Control

Infrastructure, Power and the Public



IMAGE SOURCE: WWW.UNDP.ORG

Bill Gates and other world leaders at the 77th session of the United Nations General Assembly, attending an event convened on the theme of “The Future of Digital Cooperation: Building resilience through safe, trusted and inclusive digital public infrastructure” where it was agreed to scale up efforts to build DPI.

by **PAMODI HEWAWARAVITA**

Across the Global South, Digital Public Infrastructure is being sold as a leap forward for inclusion and modern governance. But as Pamodi Hewawaravita reveals, these systems often deepen exclusion, entrench surveillance and blur the line between public good and private control.

Scan your face using a government-approved app or press your finger to a biometric reader to collect welfare payment, enroll your child in school, access a public health scheme or retrieve land records — all within seconds. On paper, it sounds like a digital utopia, especially across Asia and the Global South, where public services are often slow, opaque or out of reach.

This is the promise of Digital Public Infrastructure (DPI): to modernise governance and make interactions between the citizen and the state frictionless. But there's a catch. When the state embeds itself into the device in your pocket, it doesn't just streamline access — it can also centralise control and worsen exclusion, making resistance more difficult.

NON-NEUTRAL TECHNOLOGY

● Policymakers, big philanthropists and tech corporations are actively pitching, promoting and funding DPI. The Gates Foundation, [a major backer of DPI](#), frames it as the modern equivalent of roads and railways, enabling digital economies just as physical infrastructure once enabled the industrial age.¹ The United Nations Development Programme (UNDP) goes even further, calling DPI [“as essential in the 21st century as railways were in the 19th”](#).² In the background, corporations like Microsoft, Amazon Web Services and Google are positioning themselves to collect the tolls that governments and citizens will no doubt have to pay to use their digital infrastructure.

Digital Public Infrastructure isn't just about access — it's about who controls the systems that shape public life.

As the Global South constructs these new digital roads, the need to critically evaluate their building blocks — and the socio-political circumstances in which they operate — is increasingly urgent. These platforms aren't just conduits; they're also systems of power that are increasingly rewriting the relationship between citizen and state, often without consent or transparency. As Raman Jit Singh Chima, Access Now's Asia Pacific Policy Director and Senior International Counsel, puts it: DPI is not devoid of political context, especially in South Asia.

Look no further than India, home to the most ambitious DPI rollout in human history.

The India Stack is a set of interconnected digital platforms transforming how citizens interact with the state and the economy. At its core is Aadhaar, the world's largest biometric identification system, assigning each person a unique number linked to their fingerprints and iris scans. Aadhaar is layered with a Unified Payments Interface (UPI) for real-time mobile payments, powering billions of transactions monthly, and DigiLocker, a cloud-based digital vault allowing individuals to store, verify and share documents like tax records.

While the scale of India's DPI implementation is jaw-dropping, some of its consequences are less positive.

The elderly, the sick and the immobile — people who need government assistance the most — often find themselves locked out of the system due to biometric mismatches or connectivity issues. Rethink Aadhaar, an online platform, [documents cases of harm and even death](#) caused by the India Stack. For instance, from 2015 to 2018, Rethink Aadhaar documented twenty-five hunger deaths caused by Aadhaar-related issues. [Media reports](#) point to cases of people who were denied food rations because they'd failed to link their food ration cards to Aadhaar.³

Chima also points out that digital identities have implications for sensitive issues affecting the rights of diverse communities, religious minorities and different ethnic and linguistic groups — specifically how they're recognised (or not recognised) in a country's political system: “Whether it's about voting, citizenship or other identity-related issues, we see an increased polarisation on communal lines, sometimes across South Asia. I think we need to be very careful on where they intersperse on digital identity-based approaches to DPI.”

Worse still, India's DPI architecture has surveillance baked into its DNA. All citizens are at risk of being surveilled by the state as the Aadhaar Act [allows the sharing of demographic data and authentication records](#) — including for “national security” purposes — without clear definitions or checks.⁴ There are no strong data protection laws. No independent audits. No opt-out button.

IGNORING DISTRESS SIGNALS

● A growing number of voices are highlighting problematic aspects of DPI like Aadhaar, but they're often drowned out by influential techno-solutionist advocates who are altering the original vision of DPI on the global stage. Initially, advocates dreamt of truly public digital spaces where people would be able to freely express themselves, exchange ideas and engage in discourse without being exploited for profit. However, what started as an ideal of civic engagement in digital spaces through [community-driven, decentralised infrastructure](#) has become a narrow tunnel for economic growth.⁵

Instead of fostering civic life and supporting community-led innovation, states and profit-driven entities are more interested in building pathways for private sector growth. This has resulted in powerful governments shipping their digital governance models to their less powerful neighbours without first critically evaluating the potential harm of such transfers. For instance, China's Digital Silk Road is now [making inroads in countries in Africa and Asia](#) eager for economic opportunities — at the cost of

digital security.⁶ Meanwhile, the European Union (EU) has unveiled their '[Global Gateway](#)' strategy, promising to address the digital divide in a quest for sustainable development.⁷

Due to DPI being traded in this manner, smaller states are becoming battlegrounds for global superpowers in new ways. We can see this in Kenya, where China and the US are vying for control, notes Muthuri Kathure, a senior fellow at Tech Global Institute. On the one hand, the Kenyan government is keen on doing business with China. On the other, the US sees Kenya as a hub serving multiple purposes in trade, security and counterterrorism.

Chima encourages smaller countries to learn from the mistakes of Aadhaar — not solely from a technical perspective but also from a societal perspective. "These stories are up online. Access Now, for example, has [recommendations](#) on national digital identity programmes, where we say exactly what governments should do and not do when they deploy their own programmes.⁸ It doesn't mean that you don't build digital systems or programmes, but you ask whom is it being built for, and in what manner? And most importantly, [why are you doing it?](#)"

He notes the importance of placing human rights at the centre of DPI to ensure that digital technology empowers individuals and communities, instead of entrenching existing power structures and inequalities.

"To create truly public digital infrastructure, it is essential to prioritise the needs and rights of individuals, particularly those most vulnerable to exclusion and coercion. This requires a shift from viewing DPI as a purely technical solution to understanding it as a social process that must be governed by principles of equity, inclusion, transparency, and accountability. Digital transformation should never be an end in itself but a means to achieve broader social goals."

LOCKING IN DIGITAL COLONISATION

● As DPI crosses borders, it is increasingly being shaped by international rules and agreements. Digital Trade Agreements (DTAs) are a new class of international treaties setting the terms for how data, digital services and technologies move across borders.

Close scrutiny of DTAs reveal how these deals can seriously harm the rights of citizens. Often negotiated and signed without meaningful public consultation, DTAs can prohibit data localisation (keeping data stored within national borders), prevent mandates for open-source software, and ban disclosure of source code, undermining efforts at algorithmic transparency and public oversight. Take the EU's first standalone DTAs with Singapore and Japan, for example. One of their most concerning provisions [favours cross-border data flows](#), even when the receiving country offers much weaker protections.⁹ The DTA doesn't simply allow data to flow abroad — it also prevents the EU from stopping such transfers even when rights are endangered. For vulnerable groups like migrants, who are already subject to systemic surveillance and discrimination, this opens the door to data-driven harm with little recourse.

DPI may promise inclusion, but it often deepens exclusion and expands state and corporate power.

IS DPI REALLY ‘PUBLIC’?

● While DPI is framed as a public good — like roads or electricity — it is, in practice, frequently built, hosted and maintained by private actors, including some of the world’s most powerful corporations. Their involvement in DPI with little transparency or public oversight raises serious questions about how ‘public’ DPI really is, especially when citizens may be subject to commercial surveillance, data extraction and platform lock-in.

For example, in a move that blurs the lines between public infrastructure and commercial service delivery, [Mastercard has partnered with the Nigerian government](#) to develop a biometric digital ID and payment system.¹⁰ In Bangladesh, the government’s [national cloud infrastructure is hosted on Oracle Cloud](#), supporting critical systems for health, finance and public administration under the ‘Smart Bangladesh Vision 2041’ initiative.¹¹

The next frontier is the integration of AI into DPI. Automated decision-making is already being used to determine who qualifies for welfare, detect fraud, assign risk in healthcare and enhance policing systems. But AI technologies are prone to bias and difficult to challenge. As DPI expands, so too will its entanglement with algorithmic governance — increasing the risk of systemic discrimination at scale.

As states reimagine democracy and governance to fit the digital realm, Kathure stresses the need for genuine citizen engagement, even if it may not make “political sense” at first glance to do so. “Governments and civil society organisations are the lead actors who have the privilege to be in these spaces. We need to find a way in which they’re able to involve the people. It’s a complex conversation. People care about food, shelter and clothes. But this [DPI] is going to affect the basic needs, and so we need to find a way to talk to them about these things in the language that they understand.”

One way of bridging the gap could be through intermediaries from the community, says Shita Laksmi, a digital governance consultant. Even citizens with internet access have different digital literacy levels, so intermediaries could play important roles in helping governments educate the public.

“For example, in the health sector, we have workers who talk with pregnant women, closely monitoring their pregnancy through the nine months and ensuring they take vitamins and attend their doctors’ appointments,” Laksmi says. “These intermediaries are not part of the government, they’re part of the community and they do important work in translating issues to pregnant mothers. We need a similar system for citizens, to help governments with their DPI rollouts.”

With DPI laying the foundation for many fundamental aspects of life — from welfare and education to law enforcement — we must ask: who controls the infrastructure of our digital public life?

In many countries, limited capacity, restricted funding and competing priorities are preventing digital rights organisations from critically interrogating the techno-solutionist drive led by government officials and DPI advocates. The media is also relatively silent on the issue. It’s likely that parts of civil society and the media have already been drawn into — or captured by — the dominant digital development narrative.

While they hasten to develop cutting-edge systems, governments and contractors need to be more transparent about how those arrangements are structured. Who benefits, how is data used and can members of the public opt out if they don’t agree with the design? Ultimately, it’s up to citizens and civil society to ensure that this new world that’s being built will genuinely serve the public’s interests, instead of those of a powerful few at the top. 

WRITER BIO:

Pamodi Hewawaravita works as a Researcher at CommonEdge.Asia. She’s also a journalist, exploring stories affecting communities around Sri Lanka. When not writing, she spends her time reading, travelling around the island, or hanging out with cats.

END NOTES

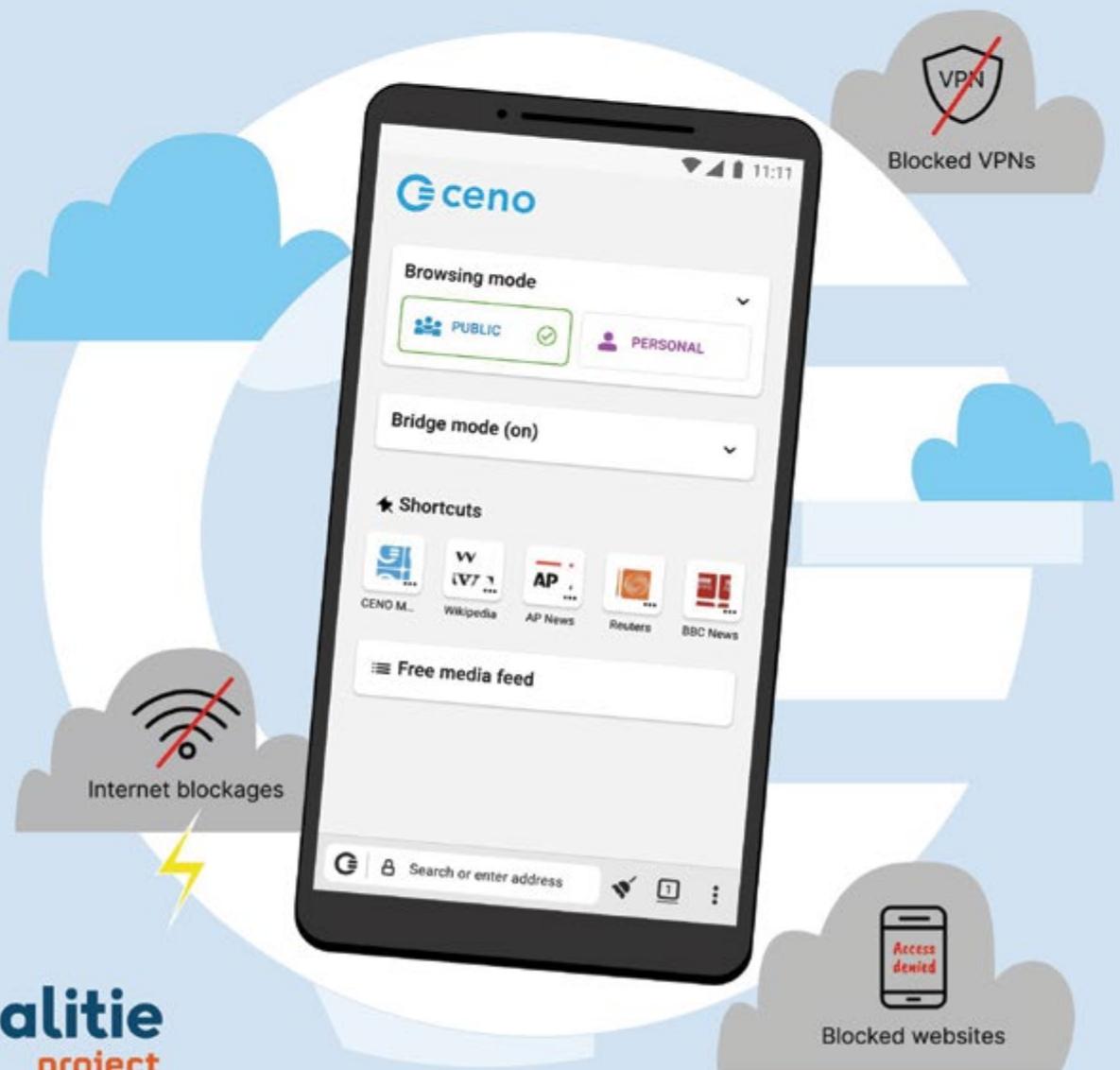
1. Digital Public Infrastructure. Gates Foundation. <https://www.gatesfoundation.org/our-work/programs/global-growth-and-opportunity/digital-public-infrastructure>
2. Why donors are backing a global push for digital public infrastructure. Catherine Cheney, Devex, 30 September 2022. <https://www.devex.com/news/why-donors-are-backing-a-global-push-for-digital-public-infrastructure-104007>
3. The link between India’s biometric ID scheme and starvation. Dharvi Vaid, Deutsche Welle, 26 March 2021. <https://www.dw.com/en/the-link-between-indias-biometric-identity-scheme-and-starvation/a-57020334>
4. Aadhaar: Enabling a form of supersurveillance. Suhrit Parthasarathy, The Hindu, 4 December 2021. <https://www.thehindu.com/opinion/lead/aadhaar-enabling-a-form-of-supersurveillance/article62112102.ece>
5. A human rights-centred approach to digital public infrastructure. Access Now, 24 October 2024. <https://www.accessnow.org/guide/digital-public-infrastructure/>
6. Assessing China’s Digital Silk Road Initiative. Council on Foreign Relations. <https://www.cfr.org/china-digital-silk-road/>
7. Global Gateway. European Commission. https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/stronger-europe-world/global-gateway_en
8. National Digital Identity Programmes: What’s Next?. Access Now, May 2018. <https://www.accessnow.org/wp-content/uploads/2019/11/Digital-Identity-Paper-Nov-2019.pdf>
9. The EU’s New Data Flow Agreements with Japan and Singapore Could Threaten Privacy Rights. Digital Trade Alliance, 9 December 2024. <https://dtalliance.org/2024/12/09/the-eus-new-data-flow-agreements-with-japan-and-singapore-could-threaten-privacy-rights/>
10. MasterCard to Power Nigerian Identity Card Program. NoCash, 8 May 2013. <https://nocash.ro/mastercard-to-power-nigerian-identity-card-program/>
11. Bangladesh gov’t equips data centers with Oracle Cloud Infrastructure. Georgia Butler, Data Center Dynamics, 8 May 2024. <https://www.datacenterdynamics.com/en/news/bangladesh-govt-equips-data-centers-with-oracle-cloud-infrastructure/>





 ceno.app

Ceno is rebuilding a borderless Internet, censorship and shutdown resistant. Over a peer-to-peer network, Ceno users browse and share web content with each other.



eQualitie
an **project**



Who Writes the Rules?

The new order of platform power



PHOTO OF A SLIDE FROM A PRESENTATION ABOUT THE EU'S DIGITAL MARKETS ACT.

US political and tech power converge, steering the global conversation on technology and governance.

by **MIRAJ CHOWDHURY**

Miraj Chowdhury examines how the Trump administration's alliance with Big Tech is reshaping not just US regulation but global digital governance – with far-reaching consequences for rights, power and accountability.

On 4 July 2025, US President Donald Trump signed into law what has come to be known as the [One Big Beautiful Bill](#). An earlier version of this bill, passed by the House in May, included [a sweeping ten-year moratorium](#) on state-level regulation of artificial intelligence models and automated decision systems.¹ Although that provision was stripped almost unanimously in the Senate, it was a reminder of the new administration's alliance with big tech companies, and of what might follow in the coming days.

Trump's intentions were clear when, within days of his inauguration, he signed [Executive Order 14179](#), titled 'Removing Barriers to American Leadership in Artificial Intelligence'. It overturned several Biden-era directives that had introduced ethical guidelines, procurement requirements and safeguards related to AI's labour and social impacts. What the previous administration framed as "necessary guardrails", the Trump administration now [characterises](#) as "unnecessarily burdensome" policies that risk stifling private sector innovation and undermining US leadership in emerging technologies.²

The order came at a time when dozens of US states were [introducing](#) hundreds of bills to regulate AI — ranging from algorithmic bias protections to deepfake bans and proposals to mitigate broader AI risks. But this was not only a shift in domestic policy. It was also a signal: that the US federal government under Trump had aligned itself with Big Tech’s ambition to reset the rules of global digital governance.

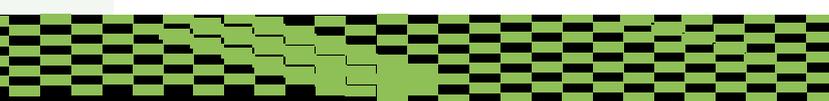
In the months that followed, the rollback of oversight was accelerated. The Federal Trade Commission (FTC) was gutted of Democratic leadership, hundreds of policy documents on AI and consumer protection were [withdrawn from public access](#)³ and Silicon Valley was formally invited to “help make government more efficient” through a new Department of Government Efficiency (DOGE).

Some Big Tech companies had been in bitter conflict with the previous administration, particularly over content moderation, pandemic misinformation and online speech. For example, Meta had grown resentful of the Biden White House’s demands to limit harmful content. [The Murthy v. Missouri case](#) crystallised the frustration that the government was coercing social media companies to police online speech related to Covid-19, vaccines and the 2020 election.⁴

For many tech leaders, the proliferation of state-level bills and the Biden administration’s regulatory stance were threats to their business models, their control over digital infrastructure and their capacity for unbridled innovation in the face of Chinese competition. The growing sense of government interference created fertile ground for an alliance with a political figure who promised to simply “leave them alone” or, better yet, clear their path. When Mark Zuckerberg [publicly admitted](#) in 2024 that Facebook had over-complied with White House pressure to suppress Covid-related satire and stories about Hunter Biden,⁵ he wasn’t just deflecting blame — it seemed like he was signalling a new alliance.

By mid-2024, the realignment was underway. Elon Musk founded the [America Super PAC](#). Andreessen Horowitz released its [‘Little Tech Agenda’](#), positioning tech deregulation as a patriotic cause. The Trump campaign was [flooded with contributions](#) from platform billionaires and crypto magnates. Meta and Amazon each donated \$1 million to Trump’s inauguration fund; OpenAI, Coinbase and PayPal followed suit. Tech leaders, once hesitant to openly back Trump, now viewed him as the president willing to help them expand.

Stemming from the US state-tech alliance, pressure for tech deregulation is likely to increase across the world.



While domestic deregulation was anticipated and has visibly taken shape over the past few months, something even more ambitious is unfolding: an effort by US tech firms, backed by the federal government, to influence legal regimes well beyond their national borders.

It looks as if the European Union will be the primary battleground, if it isn’t already. In Brussels, tech platforms are actively challenging core provisions of the EU’s Digital Services Act (DSA) and AI Act. Lobby groups including the Computer & Communications Industry Association (CCIA) have [called on](#) the EU to pause enforcement, citing “damage to innovation”.⁶ Meta and TikTok have filed legal complaints against the supervisory fee system. European NGOs warn that Washington and Silicon Valley are working together to water down Europe’s digital agenda.⁷

The rush to influence global policies is also visible in major tech platforms’ lobbying efforts. In the first quarter of 2025 alone, Google [spent \\$3.01 million](#) on lobbying while Meta [spent about \\$8 million](#) — the highest Q1 spend to date.⁸ Their filings frequently mention cross-border data flows, EU-US trade negotiations and digital regulation, highlighting concern with the General Data Protection Regulation (GDPR) and other digital laws.

The influence is not centred around one market alone. In [a recent disclosure](#), Meta reported lobbying Congress and the US Trade Representative, among others, on what it called “international digital policy” — including privacy, data localisation, content moderation and regulatory proposals — in Bangladesh, Pakistan, India and Nigeria. Google has [engaged in](#) lobbying around export controls for emerging technologies, cross-border data flows and digital trade provisions in free trade agreements, signalling a broader concern with regulatory fragmentation and data localisation trends worldwide.

In a [2025 commentary](#) for *Tech Policy Press*, Gordon LaForge, a policy analyst, argued that US tech firms have increasingly acted as foreign policy players — negotiating with governments, shaping trade norms and influencing regulation abroad.⁹ A *Tech Policy Press* series titled [‘The Coming Age of Tech Trillionaires and the Challenge to Democracy’](#) has also warned that the global influence of US tech is no longer just economic or cultural, but also legal and institutional.¹⁰ The global political impact should not be overlooked. According to [a commentary](#) published on *Foreign Policy*: “Silicon Valley is becoming an instrument of U.S. coercion, and that’s a danger to each and every country”.¹¹

The global consequences of this influence aren’t just shaped by policies, but also by where they land. In the EU, strong institutions and independent courts can enforce user protections in a better way. But in an increasingly authoritarian world, the same regulatory tools — like data localisation mandates or content takedown laws — can be repurposed for surveillance, repression and political control, depending on governance and political environment. A policy that protects users in Brussels can chill dissent in Dhaka or Lagos.

This is why, for people in many of these countries, legislation can be a double-edged sword. On the one hand, less regulation might mean more freedom, but it also means ceding more power to unaccountable corporations. On the other, demanding more regulation may lead to censorship and repression. Where institutions are weaker, civil society is under pressure, and enforcement is often politically captured, the same influence from platforms — reinforced by US backing — may tilt digital policy even further toward corporate or state interests. The result may be weakened user protections.

This raises several critical questions for countries in Asia, Africa, Latin America and the Middle East. As we increasingly live within the infrastructure, rules and norms set by big tech companies — without the bargaining power to influence their decisions — who defends the rights of users? Does the state-tech alliance mean a drastic shift from rights to power? Will states demand more control over content in return for letting tech giants shape the future of AI and commerce? And, most importantly, what happens when these dynamics intersect with geopolitics?

During the recent India–Pakistan conflict, in [a sign of sweeping censorship](#), over 8,000 accounts — including those of journalists, creators and news outlets from India, Pakistan, Bangladesh, China and Turkey — were blocked on X within Indian territory.¹²

YouTube [geoblocked](#) Pakistani and Bangladeshi news channels in India; Pakistan retaliated by banning Indian digital content. This spiral of platform-enforced censorship raises urgent questions about whether companies, lobbying to shape laws, are also becoming too willing to carry out political takedowns in return for regulatory favor.

No matter how the coming years unfold, there will likely be more pressure for tech deregulation across the world, coming from the US state–tech alliance. The impact of this on countries and their people will almost certainly be uneven. In much of the world, the protections you enjoy online — over your speech, data, safety — will increasingly depend on where you live, who governs you and how much revenue platforms see in your market.📍

WRITER BIO:

Miraj Chowdhury is the founder of Digitally Right in Bangladesh, focusing on the intersection of media, technology, and society. With nearly 18 years of experience in journalism, research, and media development, he has worked as a regional editor at the Global Investigative Journalism Network and served as an adjunct faculty teaching journalistic research. Miraj is a 2020 GNI-Internews Digital Rights Fellow and sits on the boards of MRDI and What To Fix.

END NOTES

1. No state AI law moratorium in One Big Beautiful Bill Act. Reuben Bank and Dale C. Van Demark, *McDermott Will & Schulte*, 8 July 2025. <https://www.mwe.com/insights/no-state-ai-law-moratorium-in-one-big-beautiful-bill-act/>
2. Trump Administration Unveils New AI Policy, Reverses Biden’s Regulatory Framework. Danielle Ochs, Jennifer Betts, Zachary V. Zaggar, *The National Law Review*, 7 February 2025. <https://natlawreview.com/article/trump-administration-unveils-new-ai-policy-reverses-bidens-regulatory-framework>
3. Trump 2.0 Tech Policy Rundown: 100 Days in, Federal Agencies Shift AI, Privacy, and Governance Priorities. Omer Tene and Reema Moussa, *Goodwin Procter*, 7 May 2025. <https://www.goodwinlaw.com/en/insights/publications/2025/05/insights-technology-dpc-trump-tech-policy-rundown-100-days>
4. Justices side with Biden over government’s influence on social media content moderation. Amy Howe, *SCOTUS Blog*, 26 June 2024. <https://www.scotusblog.com/2024/06/justices-side-with-biden-over-governments-influence-on-social-media-content-moderation/>
5. Meta CEO admits Biden–Harris admin pressured company to censor Americans. Greg Wehner, *FOX Business*, 26 August 2024. <https://www.foxbusiness.com/politics/meta-ceo-admits-biden-harris-admin-pressured-company-censor-americans>
6. Tech lobby group urges EU leaders to pause AI Act. *Reuters*, 26 June 2025. <https://www.reuters.com/technology/tech-lobby-group-urges-eu-leaders-pause-ai-act-2025-06-25/>
7. Europe ‘must not be bullied’ by Trump and Musk on tech laws, NGOs say. Jennifer Rankin, *The Guardian*, 29 January 2025. <https://www.theguardian.com/world/2025/jan/29/europe-must-not-be-bullied-by-trump-and-musk-on-tech-laws-ngos-say>
8. According to reports on lobbying activity filed by Google and Meta in accordance with the Lobbying Disclosure Act. Reports can be found at <https://lda.senate.gov/system/public/>
9. Big Tech’s Foreign Policy Takeover. Gordon LaForge, *Tech Policy Press*, 2 May 2025. <https://www.techpolicy.press/big-techs-foreign-policy-takeover/>
10. The Coming Age of Tech Trillionaires and the Challenge to Democracy. *Tech Policy Press*. <https://www.techpolicy.press/category/the-coming-age-of-tech-trillionaires-and-the-challenge-to-democracy/>
11. Big Tech Is a Tool of Trump’s Global Disruption. Misha Glenny and Robert Muggah, *Foreign Policy*, 3 June 2025. <https://foreignpolicy.com/2025/06/03/trump-big-tech-companies-silicon-valley-threat-geopolitics-digital-sovereignty/>
12. How India and Pakistan’s Digital Authoritarianism Sows the Seeds of War. Shumaila Hussain Shahani and Disha Verma, *The Diplomat*, 18 June 2025. <https://thediplomat.com/2025/06/how-india-and-pakistans-digital-authoritarianism-sows-the-seeds-of-war/>



"Show Us Your Screens"

Algorave and the radical joy of live coding

by PRARTHANA MITRA



Screengrab from estuary jamming beatnyk (Padmanabhan J.) an opheliagame (Anushka Trivedi) from YouTube, February 2025.

Part rave, part code jam, part resistance — algorave is a global counterculture movement transforming laptops into instruments of liberation. Emerging from the open-source live coding community, algorave artists make their process visible in real time, challenging the black-boxed dominance of Big Tech. From India to Indonesia, creative coders and collectives, with rising participation of women and queer folks, are remixing dance music, education and tech politics — not only imagining a more just digital future but also performing it. Prarthana traces algorave's sonic manifesto and its defiant call: make the code public, make the culture shared, and make the dance floor political again.



The message on the wall, a deceptively simple call to unhide what's on our screens, reads almost like a command for the "[Big Daddy Mainframe](#)" of surveillance tech (which would make this a rather odd provocation to introduce in an anthology about/against digital power). But it's really more of a commandment to resist technological black-boxing, and its origins lie in the open-source live coding community.

A burgeoning global counterculture movement against tech obscurantism, algorave — short for algorithmic rave — involves writing code to make live music (or other time-based art like visuals or choreography). This form of creative labour is not only taking dance music back to its radical roots but also powering a critical questioning of the Big Tech industrial complex through a performance of something that's typically inscrutable — the code.

If we look back at [Synchrony](#), a short film made by Norman McLaren in 1971, we encounter something of a prototype for elaborate and self-reflexive multidisciplinary approaches to interrogate and interact with the structure constituents that make, well, *life*. In *Synchrony*, McLaren makes sound visible by taking apart the apparatuses of audiovisual production and breaking them into units of light, colour, shape and rhythm.

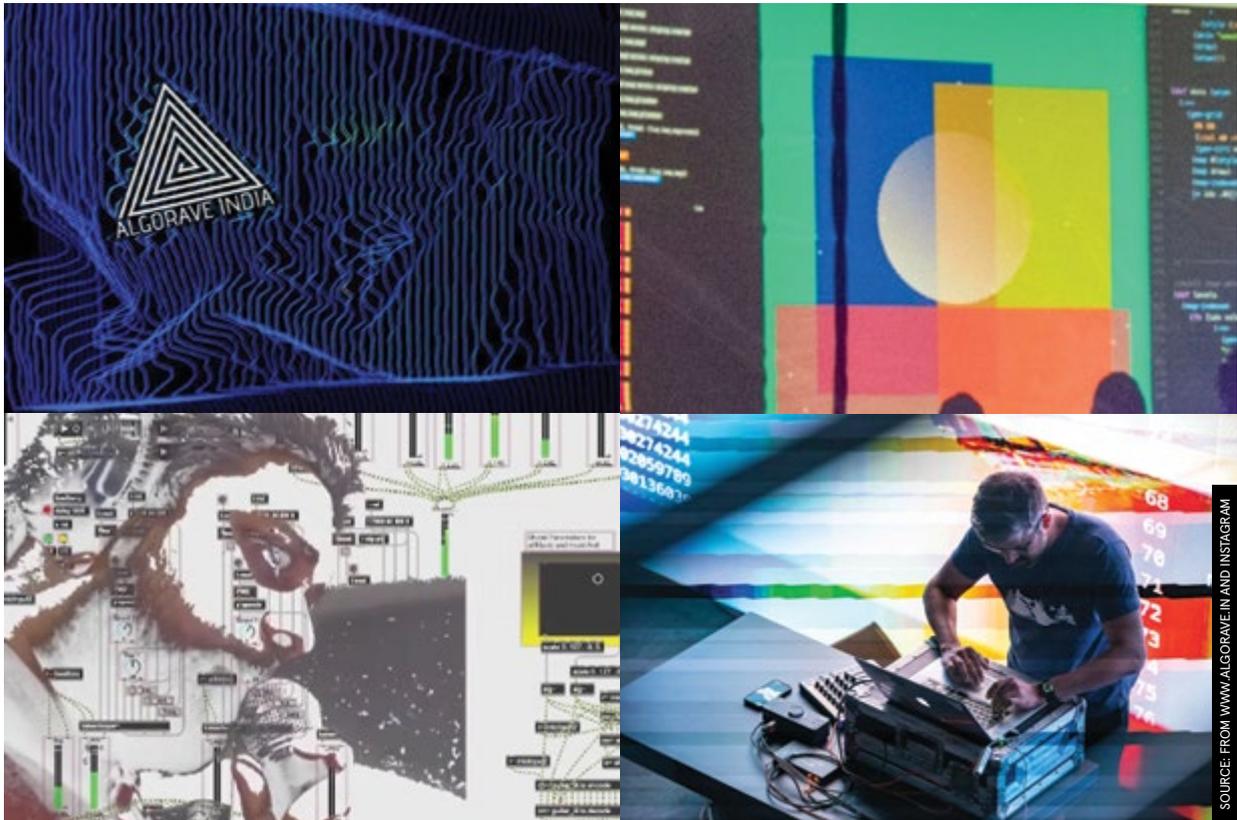
In 2004, an emerging crop of internet artists in Sheffield in the United Kingdom did something similar. They were led by Alex McLean, who had the foresight to pre-emptively address what has now emerged as critical pain points in computational tech regulation and accountability — namely, the black-boxing and gatekeeping of code and data. They introduced a form of sound art performance that, as the independent magazine *The Wire* [put it](#), is "all about getting into the guts of how music is made, showing code running in real time, taking machines and systems apart to show their workings and opening up technologies to alternative uses".¹

Precisely because technological systems produce paranoid subjects out of us by controlling and restricting the information we get, the [TOPLAP manifesto](#) and *Live Coding: A User's Manual* — two documents that have fuelled the algorave movement — both emphasise the need to make algorithms visible in order to better understand, subvert, reappropriate and play with them.² And play they did, bringing together live coding enthusiasts from across the world to computer music parties, design sprints and hackathons. These became spaces where hacker philosophy, geek culture and clubbing collapsed, each with varied manifestations of its own but still organising themselves around the same central philosophies. What emerges is the paradigm of a participant-audience.

This form of creative labour is not only taking dance music back to its radical roots but also powering a critical questioning of the Big Tech industrial complex through a performance of something that's typically inscrutable — the code.

An overlooked but pivotal aspect of algorave is the centrality of collaboration, likely a natural extension of the movement's championing of open-source technologies like [TidalCycles](#), [Sonic Pi](#), [SuperCollider](#) and [p5.js](#). Whether it's decolonising technology, technology education or electronic dance music, it must all begin with decolonising the software, and the way these programming instruments are used to build communities of practice. These musicians recognised that.

In the twenty-five years since it came into being, the algorave movement has brought together and encouraged hundreds of musicians, artists and researchers to start their own dedicated nodes and instigators across the global majority today. These creators are now taking and interpreting this vision for democratising access and knowledge to tinker with code in their own contexts. These nodes are not only connected to each other through [virtual showcases and exchanges](#) but have also each made great strides in incubating young artists in their respective contexts. As a result, the sounds of algorave today encompass a range of styles: from minimal techno and [live-coded ragas](#) to "cinging" (coding + singing). But no matter how much they differ, all these styles are unified in the calculated rawness of their transmissions.



Screengrab from TOPLAP 20 Stream featuring eardrummerman (manaswi) from YouTube, February 2024.

The Global South boasts a diverse and growing community of algorave performers and live coding enthusiasts, instigated by Algorave India’s Abhinay Khoparzi, Akash Sharma, Dhanya Pilo and Joshua Thomas, Pakistan-based Karachi Community Radio’s Jahanzeb Safder, Indonesia’s Rangga Purnima Aji, Argentina’s Iris Saladino and Colombia’s Alexandra Cardenas — to cite a few — all with unique contours and agendas framed by the digital landscape in their respective contexts. Their sets are strewn with digital artefacts that are singular to each location and the artist’s own identity: hyperlocal memes and news footage, musical instruments and sounds, even topographical references like ‘estuary sessions’ — all play the dual role of reliability and representation.

Challenging what critic Hubert Adjei-Kontoh [describes](#) in *The Baffler* as the “defanged, neatly packaged identity politics of dance music”, algorave builds liminal spaces which allows anyone with a laptop and a fundamental understanding of computational processes to make music.³ Importantly, it also educates and empowers the audience to become an active participant in bearing witness to the making of an audio story.

**These became spaces
where hacker
philosophy, geek culture
and clubbing collapsed**

When it comes to representation in algorave, the practice of live coding as a means of expression and resistance is, to a great extent, still restricted to urban centres. This is especially true in a country like India, where access to the internet, hardware and a community is still prescribed by power imbalance and systemic inequalities. But recent trends — particularly owing to mass curiosity and awareness around generative AI and readily accessible tools — portend to the mainstreaming of algorave in the future.



An overlooked but pivotal aspect of algorave is the centrality of collaboration, likely a natural extension of the movement's championing of open-source technologies

Allahabad-based Khoparzi, one of the earliest algoravers from India, recognised the merit in situating the movement in India as an art collective that promotes programming as a performance art. Founded in 2018, Algorave India has since evolved into a “strategy for community development, music education, computational literacy”.⁴ Several promoters are now using it as a pedagogical tool and making great strides towards leveraging creative coding’s potential to start important conversations, particularly among data workers and STEM aspirants about the possibilities of open-source tech, the advantage of multidisciplinary approaches in coding practice, and the real-world implications of the black-boxed technologies they’re trained to build/refine/test.

The work to meaningfully centre the most marginalised, surveilled and othered bodies in this movement has begun with the sprouting of, for example, women’s coding collectives like Ajaibghar. Based out of Rajasthan, Ajaibghar artists like Ambika Joshi, Nanditi Khilnani and Anushka Trivedi explore emotional experiences, motherhood and self-care through generative music, poetry and art. They also provide space for women to participate in creative computation through initiatives like [Coding with Friends](#). The now-defunct Coven Code — which comprised many algoravers based out of New Delhi — was also set up to onboard and orient more women and gender diverse people into live coding, create safer dance floors for women, and reclaim technology. There is much resonance with the VNS Matrix, which emerged from the [Cyber-feminist Manifesto](#) to “hijack the toys from technocowboys and remap cyberculture with a feminist bent”.⁵

In its liberatory playfulness, algorave transcends “reimagination” as merely a discourse and actually reimagines another world that may exist within the paradigm of Donna Haraway’s “polymorphous information system” — a concept that describes a flexible, interconnected network of humans, machines and meanings, where boundaries are blurred and multiple realities can coexist. At the same time, it is still able to abandon the master’s [proprietary] tools in lieu of open tech systems. Like with any counterculture, algorave, too, thrives on volunteers and vanguards who form an ecosystem. In India, art curators, F/LOSS (Free/Libre and Open Source Software) communities, sound artists, AR/VR studios, programmers and design practitioners are all collectively conceiving new and contextually rooted ways of bringing a (b) rave new world into being. They do this by primarily changing the conditions under which art and algorithms come into meaning. As audience-participants, we can only bring our curiosities and openness — to bear witness, to keep the code running. 

WRITER BIO:

Prarthana (they/them) is interested in exploring third spaces through their feminist research and creative communications practice at the intersection of bodies, tech and justice. A 2024 DRAPAC Fellow, Prarthana’s work in the digital rights space has involved organising digital communities of practice and designing campaigns, games and interventions around gendered disinformation, platform accountability and decolonial AI. Prarthana has also written on policy and culture, particularly audio practices in South Asia, for Wild City, Gaysi and Border Movement. Currently, they are building a digital project around chronic disabilities out of Goa, India.

END NOTES

1. mily Bick visits AlgoMech Festival in Sheffield. Emily Bick, *The Wire*, December 2017. <https://www.thewire.co.uk/in-writing/essays/emily-bick-visits-algomech-festival-in-sheffield>
2. ManifestoDraft. TOPLAP. <https://toplap.org/wiki/ManifestoDraft>; Live Coding: A User’s Manual. Edited by Alan F. Blackwell, Emma Cocker, Geoff Cox, Alex McLean, Thor Magnusson, MIT Press, 2022.
3. Dance Dance Revolution? Hubert Adjei-Kontoh, *The Baffler*, April 2024. <https://thebaffler.com/salvos/dance-dance-revolution-adjai-kontoh>
4. About. Algorave India. <https://algorave.in/pages/about.html>
5. Feminist Worldbuilding in the Australian Cyberswamp. Claire L. Evans, *Rhizome*, 27 October 2016. <https://rhizome.org/editorial/2016/oct/27/cyberfeminist-worldbuilding/>



CONTRIBUTE TO BALANCE

We're always looking for fresh perspectives, powerful ideas, and creative voices to feature in Balance.

Whether you're a journalist, writer, artist, researcher, activist, or someone reimagining technology and its role in shaping our future, we want to hear from you. If your work connects with the themes we explore - from technology and culture to society and the planet - we'd like to meet you and start a conversation.

**Scan the QR code to share your details
and tell us how you'd like to be involved.**

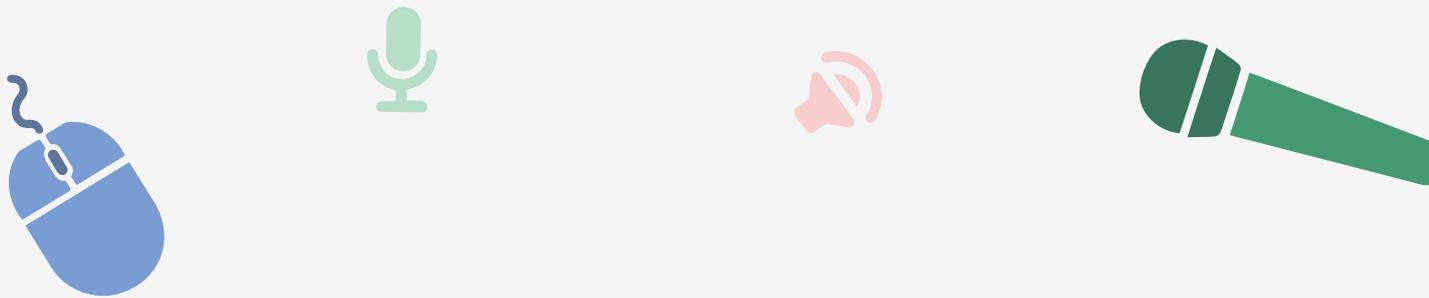


<https://balance.commonedge.asia/contribute/>



DRAPAC VPN Project

FREE blocking-resistant VPN access



The DRAPAC VPN Project is designed to resist blocking by internet censors. Its decentralised structure keeps data under users' control, enhancing privacy and security, unlike centralised commercial VPNs that store data on company servers and may expose it to third parties.

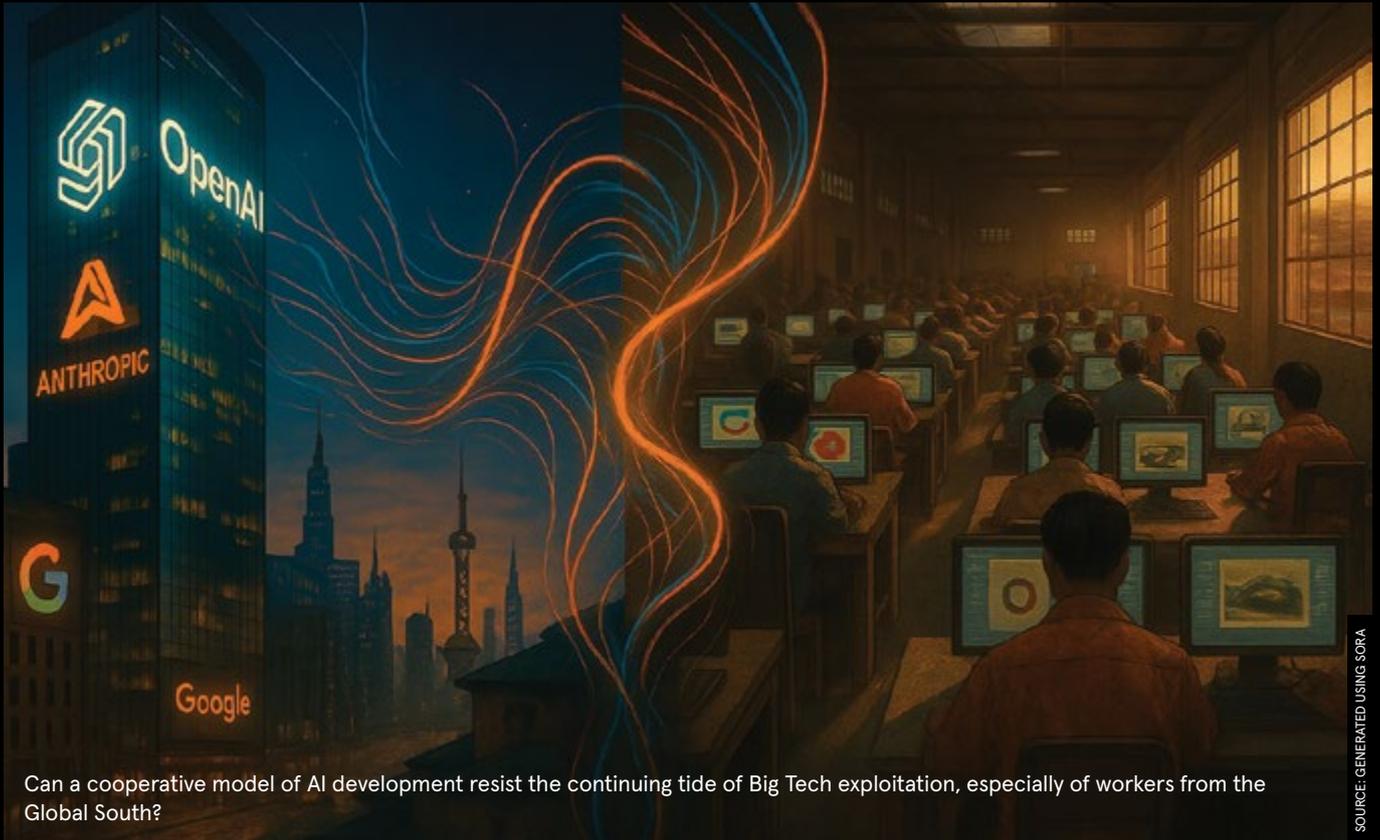
Through the DRAPAC VPN Project, we provide FREE VPN support, empowering human rights defenders to bypass online censorship and protect themselves from digital surveillance.

For more visit <https://drap.ac/vpn/>
or scan this QR code.



A Just Transition to an AI Future

Pursuing a labour-first AI agenda



Can a cooperative model of AI development resist the continuing tide of Big Tech exploitation, especially of workers from the Global South?

SOURCE: GENERATED USING SORA

by **RANJITHA KUMAR AND VINAY NARAYAN**

As debates over AI safety, ethics and regulation intensify, Ranjitha Kumar and Vinay Narayan examine how Global South actors are carving out their own approaches – not by trying to win the AI arms race but by reimagining the game entirely. From cooperative models of data governance to region-specific infrastructure and labour-first frameworks, they explore a powerful alternative to tech monopolies and digital dependency.

A global “[AI arms race](#)” is underway.¹ It’s so far been dominated by select technology companies from either China or the US, giving these countries a significant advantage. Tech monopolies — particularly companies like Google, Meta, Amazon, Microsoft and OpenAI — have led the charge in building Large Language Models like ChatGPT, now embedded seamlessly into everyday sociotechnical realities. We’re being catapulted towards a future featuring the extensive integration of [Artificial General Intelligence \(AGI\)](#).²

Not everyone can compete in this race. It takes massive amounts of computational power to build and run AI; one needs a large number of Graphics Processing Units (GPUs), a robust cloud infrastructure and numerous energy-intensive data centres. Approaches vary on the regulation front: while China favours [administrative regulation](#), the EU has taken a more [rules-based approach](#).³ Meanwhile, AI regulation in the US is subject to executive action, shifting based on the leanings of the president. Once in office, President Donald Trump signed executive orders that rolled back many of his predecessor's AI policies, blasting them as "[woke Marxist lunacy](#)".⁴

Economies in the Global South are generally falling behind — there's a lack of resources, from GPUs and data centres to the local talent required to develop cutting-edge AI technologies. But this doesn't mean they're untouched by the AI arms race: with the presence of cheap labour and poor enforcement of labour regulations, these jurisdictions are seen as perfect for the [pre-carious but vital data work](#) necessary for AI development.⁵ Today's AI value chain paints a clear picture, drawing a stark line between the Global North and the Global South when it comes to AI development, training and deployment — [reinforcing colonial hierarchies](#) of knowledge production and ownership.⁶

THE PLAY FOR DIGITAL SOVEREIGNTY

► Not everyone wants to compete in the race. Across the Global South, a growing movement is questioning the need to build large models to drive development, preferring to advocate and build smaller, purpose-specific models and applications. Unlike AGI, Applied AI places a greater emphasis on [applicability and relevance](#).⁷ In the Global South, innovators are [building lightweight, frugal AI applications](#) that can not only have immediate impact but also reduce dependency on the tech giants of the Global North.⁸

Today's AI value chain draws a stark line between the Global North and the Global South when it comes to AI development, training and deployment — reinforcing colonial hierarchies of knowledge production and ownership.

The idea of digital sovereignty — a nuanced play for digital power — isn't new. But AI's momentum has seen a reframing of this push to also include AI sovereignty. For the EU, this has meant wresting control over the data in the EU (through the EuroStack) away from American corporations, building resilience at the infrastructure level and building safe, trustworthy AI in the EU itself.

The notion of sovereignty has also captured the Indian imagination, particularly when it comes to building a just digital economy. [Aadhaar](#), India's digital identification system, was launched in 2009; it provides the foundational layer for the country's digital infrastructure, known as India Stack.⁹ With the integration of a Unified Payments Interface (UPI) in 2016 that revolutionised real-time money transfers, the development of India's digital public infrastructure has aided in conceptualising a Global South vision for digital sovereignty — characterised by low-cost innovations, modularity and, on occasion, [contradictory goals](#).¹⁰

The movement towards indigenously developed, purpose-specific models points in a promising direction for developing economies to invest in low-cost AI solutions with high payoffs, while reducing reliance on hegemonic powers. But while this strategy for digital sovereignty might help one's position in the AI race, it doesn't promise a future of equitable, people-centric AI development. In India, the ousting of international players from its digital ID development [bolstered](#) the might of Indian tech giants as both key infrastructure providers and benefactors.¹¹

In other cases, there might not even be viable local options: many Global South countries struggle to be self-sufficient when it comes to such high-level technology and therefore have to balance their desire for a sovereign digital future with the realities of a skewed resource landscape. This challenge was thrown into stark relief in early 2025, when the Trump administration's [sudden gutting of the US government](#) and freeze on foreign aid funding triggered a crisis of confidence in US-based technology and a renewed desire to seek — or build — alternatives.¹²

A PITCH FOR COOPERATIVE AI

► In this context, [a cooperative model of AI development](#) can help resist the tide of Big Tech dominance: by using community-centric frameworks to determine [a labour-first AI agenda](#) and promoting regional cooperation among developing nations, cooperative AI can usher in a more equitable AI future in Asia.¹³ Starting from a community-centric participatory model for voluntary data sharing — where a data cooperative can serve as an ideal economic model — this paradigm can be extended to national and regional frameworks for sharing resources, computational power and talent to bolster Asia’s ability to navigate and build binding frameworks for AI safety, governance and regulation.

Central to cooperative AI are collective frameworks of data justice, participation and value redistribution. The notion of a cooperative model for AI draws from [long-standing investigations](#) and [practical engagements](#) with bottom-up data stewardship structures.¹⁴ These intermediary structures mediate data flows on behalf of communities that comprise them, embodying principles of collective decision-making, equity and fairness.

A cooperative structure is well-suited for all stages of AI, from dataset creation and labelling to model training and deployment. Embedding cooperative principles into the AI lifecycle has the potential to redistribute power, value and ownership, and also drive agency over data and infrastructure. A statutory recognition of bottom-up data rights can be transformative for the future of AI in the Global South, not only allowing groups from the margins the power to determine where and how [co-generated data](#) is being used by Big Tech, but also boosting the development of purpose-specific models that solve [ongoing developmental challenges](#) to meaningfully bridge the digital divide.¹⁵ Additionally, cooperative and federated governance models can result in equitable participation from citizens to ensure that AI tools are being deployed with [sufficient guardrails](#) — recognising that it’s [not just about maximising AI opportunities but also minimising AI harms](#).¹⁶

A [labour-first AI paradigm](#) can better compensate workers through structural frameworks of redistribution in the form of repayment or royalties, while also enhancing Global South data workers’ collective bargaining power to demand labour and occupational safety standards.¹⁷

BALANCING REGULATION AND INNOVATION

► As the role of AI grows increasingly key to developmental gains, a unique opportunity for multilateral cooperation emerges. If such cooperation can be driven by principles of workers’ cooperativism to foster resource-sharing and establish regional standards for safety, the Global South would be in a better position to resist [AI colonialism](#).¹⁸

The groundwork for envisioning cooperative paradigms for an equitable Fourth Industrial Revolution has already begun in the Global North: [the Framework Convention on Artificial Intelligence](#) is a seminal multilateral treaty on AI, with over

fifty countries committing to aligning AI deployment with democratic values and addressing the risks of algorithmic discrimination and threat to public institutions.¹⁹

The Asia-Pacific is ripe for such regional cooperation: it already has countries with frugally designed digital public infrastructure and interoperable data frameworks for secure financial cross-border data flows. Singapore and New Zealand, along with Chile, have also signed a digital trade agreement to create a framework for a shared digital economy. The difference in resource distribution across the region has so far been seen as a disadvantage, but cooperative trade and creative financial assistance policies can enable resource-sharing across the AI value chain. Region-specific GPU trade and assistance can significantly improve the computing capacity of many countries in the Asia-Pacific, while the export of digital infrastructure tech stacks can enable not only cheaper innovation but also create opportunities for regional standards for interoperability.

Some efforts to cooperate are already underway: the [ASEAN Digital Master Plan 2025](#) is a prominent step towards achieving inexpensive innovation through regional cooperation, with commitments — inspired by the success of the EU’s General Data Protection Regulation (GDPR) — to produce regional-level guidelines for data-sharing in the region.²⁰

For AI to truly benefit everyone, a labour-first paradigm entring justice is essential, ensuring better compensation and enhanced collective bargaining power for data workers.

PURSUING A NEW GLOBAL AI DEAL

► Current regional cooperation frameworks are rife with unequal power dynamics, exacerbating debt and inequity.²¹ Despite the formation of key international initiatives — such as the Global Partnership on Artificial Intelligence (GPAI) and the OECD AI Policy Observatory — that drive for bilateral, cooperative agreements for AI, development and deployment continues to be skewed, prioritising innovation for the Global North often at the cost of developing economies.

We must envision a renewed form of economic cooperation based on principles of data and economic justice, pursuing instruments such as a binding global AI compact that follows up on the United Nations' [Global Digital Compact](#), enacted through principles of cooperativism.²² Key multilateral instruments must recognise the global digital divide and establish appropriate financial and regulatory frameworks, borrowing from the ethos of the UN Capital Developmental Fund to offer an equalised platform for the global majority. Labour justice must be at the centre of all our efforts for a just transition to a future where AI can benefit everyone. 

WRITER BIO:

Ranjitha Kumar is a Senior Research Associate at Aapti. Her work at Aapti focuses on equitable data and AI governance models. Her interests include exploring the political economy of labour and digital capitalism and examining data flows within the digital value chain. Her current research at Aapti explores critically examining data sovereignty as response to Big Tech and Big AI.

Vinay Narayan is a Senior Manager at Aapti. He leads Aapti's work on data stewardship and structures for bottom-up data sovereignty — where the current focus is on building networks of support for bottom-up data initiatives in the Global South. He is also the co-lead of Aapti's AI research practice that examines the impact of AI technologies on livelihoods and rights frameworks that can address ongoing and potential impacts.

END NOTES

1. Arms Race or Innovation Race? Geopolitical AI Development. Stefa Schmid, Daniel Lambach, Carlo Diehl and Christian Reuter, *Geopolitics*, 28 January 2025. <https://www.tandfonline.com/doi/full/10.1080/14650045.2025.2456019>
2. Magma: A Foundation Model for Multimodal AI Agents. Jianwei Yang, Reuben Tan, Qianhui Wu, Ruijie Zheng, Baolin Peng, Yongyuan Liang, Yu Gu, Mu Cai, Seonghyeon Ye, Joel Jang, Yuquan Deng, Lars Liden and Jianfeng Gao, 2025. <https://microsoft.github.io/Magma/>
3. racing the Roots of China's AI Regulations. Matt Sheehan, Carnegie Endowment for International Peace, 27 February 2024. <https://carnegieendowment.org/research/2024/02/tracing-the-roots-of-chinas-ai-regulations>; EU AI Act: first regulation on artificial intelligence. European Parliament, 8 June 2023. <https://www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence>
4. Trump signs executive orders targeting 'woke' AI models and regulation. Nick Robins-Early and Lauren Gambino, *The Guardian*, 24 July 2025. <https://www.theguardian.com/us-news/2025/jul/23/trump-executive-orders-woke-ai>
5. The digital labour of artificial intelligence in Latin America: a comparison of Argentina, Brazil, and Venezuela. Paola Tubaro, Antonio A. Casilli, Mariana Fernández Massi, Julieta Longo, Juana Torres Cierpe and Mathews Viana Braz, *Globalizations*, 19 February 2025. <https://www.tandfonline.com/doi/full/10.1080/14747731.2025.2465171?src=exp-la>
6. Artificial Intelligence in the Colonial Matrix of Power. James Muldoon and Boxi A Wu, *Philosophy & Technology*, 15 December 2023. <https://link.springer.com/article/10.1007/s13347-023-00687-8>
7. AGI vs. AAI: Grassroots Ingenuity and Frugal Innovation Will Shape the Future. Akash Kapur, *Tech Policy Press*, 27 June 2025. <https://www.techpolicy.press/agi-vs-ai-grassroots-ingenuity-and-frugal-innovation-will-shape-the-future/>

8. Building Good Digital Sovereignty Through Digital Public Infrastructures And Digital Commons In India And Brazil. Luca Belli, SSRN, 29 October 2024. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4966348
9. Aadhaar: A Unique Identity for the People. Ministry of Electronics & IT, 24 October 2024. <https://www.pib.gov.in/PressReleasePage.aspx?PRID=2067940>
10. Convergence or Conflict?: Digital Identities vs. Citizenship Rights: Case Study of Unique Identification Number, Aadhaar, in India. Nidhi Vij Mali and Martha A. Avila-Maravilla, *ICEGOV '18*, 4 April 2018. <https://dl.acm.org/doi/abs/10.1145/3209415.3209487>
11. UIDAI gave undue favour of Rs 4.92 crore to Wipro: CAG. *The Times of India*, 2 August 2016. <https://timesofindia.indiatimes.com/tech-news/uidai-gave-undue-favour-of-rs-4-92-crore-to-wipro-cag/articleshow/53507588.cms>
12. Why the world is looking to ditch US AI models. Eileen Guo, *MIT Technology Review*, 25 March 2025. <https://www.technologyreview.com/2025/03/25/1113696/why-the-world-is-looking-to-ditch-us-ai-models/>
13. Cooperative Paradigms for Artificial Intelligence. Sarah Hubbard, ASH Center for Democratic Governance and Innovation, 20 November 2024. <https://ash.harvard.edu/resources/cooperative-paradigms-for-artificial-intelligence/>; Public AI Network. Public AI. <https://publicai.network/>
14. Enabling Data Sharing for Social Benefit Through Data Trusts: Data Trusts in Climate. The Global Partnership on Artificial Intelligence, March 2022. <https://gpai.ai/projects/data-governance/enabling-data-sharing-for-social-benefit-through-data-trusts-in-climate.pdf>; The Journey of Enyorata Loviluku Women's Group: a Data Co-op in Action. Sushmitha Viswanathan, Aapti Institute, 23 March 2024. <https://aapti.in/blog/the-journey-of-enyorata-loviluku-womens-group-a-data-co-op-in-action/>
15. From co-generated data to generative AI: New rights and governance models in digital ecosystems. Joe Massey, Elena Simperl, Vinay Narayan, Avani Airan and Astha Kapoor, Open Data Institute, 5 December 2024. <https://theodi.org/insights/reports/from-co-generated-data-to-generative-ai-new-rights-and-governance-models-in-digital-ecosystems/>; Global Goals, Local Realities: Aligning AI Governance with Inclusion. Amaj Rahimi-Midani, *Tech Policy Press*, 23 May 2025. <https://www.techpolicy.press/global-goals-local-realities-aligning-ai-governance-with-inclusion/>
16. Beyond Safe Models: Why AI Governance Must Tackle Unsafe Ecosystems. Ludovic Terren, *Tech Policy Press*, 1 May 2025. <https://www.techpolicy.press/beyond-safe-models-why-ai-governance-must-tackle-unsafe-ecosystems/>; Why We Need a Global AI Compact. Amian Mohanty, Carnegie Endowment for International Peace, 1 March 2024. <https://carnegieendowment.org/posts/2024/03/why-we-need-a-global-ai-compact>
17. Can We Have Pro-Worker AI?: Choosing a path of machines in service of minds. Daron Acemoglu, David Autor and Simon Johnson, Centre for Economic Policy Research, October 2023. https://cepr.org/system/files/publication-files/191183-policy-insight_123_can_we_have_pro_worker_ai_choosing_a_path_of_machines_in_service_of_minds.pdf
18. Tech Imperialism Reloaded: AI, Colonial Legacies, and the Global South. Salvador Santino Regilme, *E-International Relations*, 17 February 2025. <https://www.e-ir.info/2025/02/17/tech-imperialism-reloaded-ai-colonial-legacies-and-the-global-south/>
19. The Framework Convention on Artificial Intelligence. Council of Europe, 5 September 2024. <https://www.coe.int/en/web/artificial-intelligence/the-framework-convention-on-artificial-intelligence>
20. ASEAN Digital Master Plan 2025. Association of Southeast Asian Nations, 2025. <https://asean.org/book/asean-digital-masterplan-2025/>
21. Is Free Trade "Free"? Is It Even "Trade"? Oppression and Consent in Hemispheric Trade Agreements. Frank J. Garcia, *Seattle Journal for Social Justice*, May 2007. <https://digitalcommons.law.seattleu.edu/cgi/viewcontent.cgi?article=1605&context=sjsj>
22. Global Digital Compact. United Nations. <https://www.un.org/global-digital-compact/en>



Navigating the Labyrinth

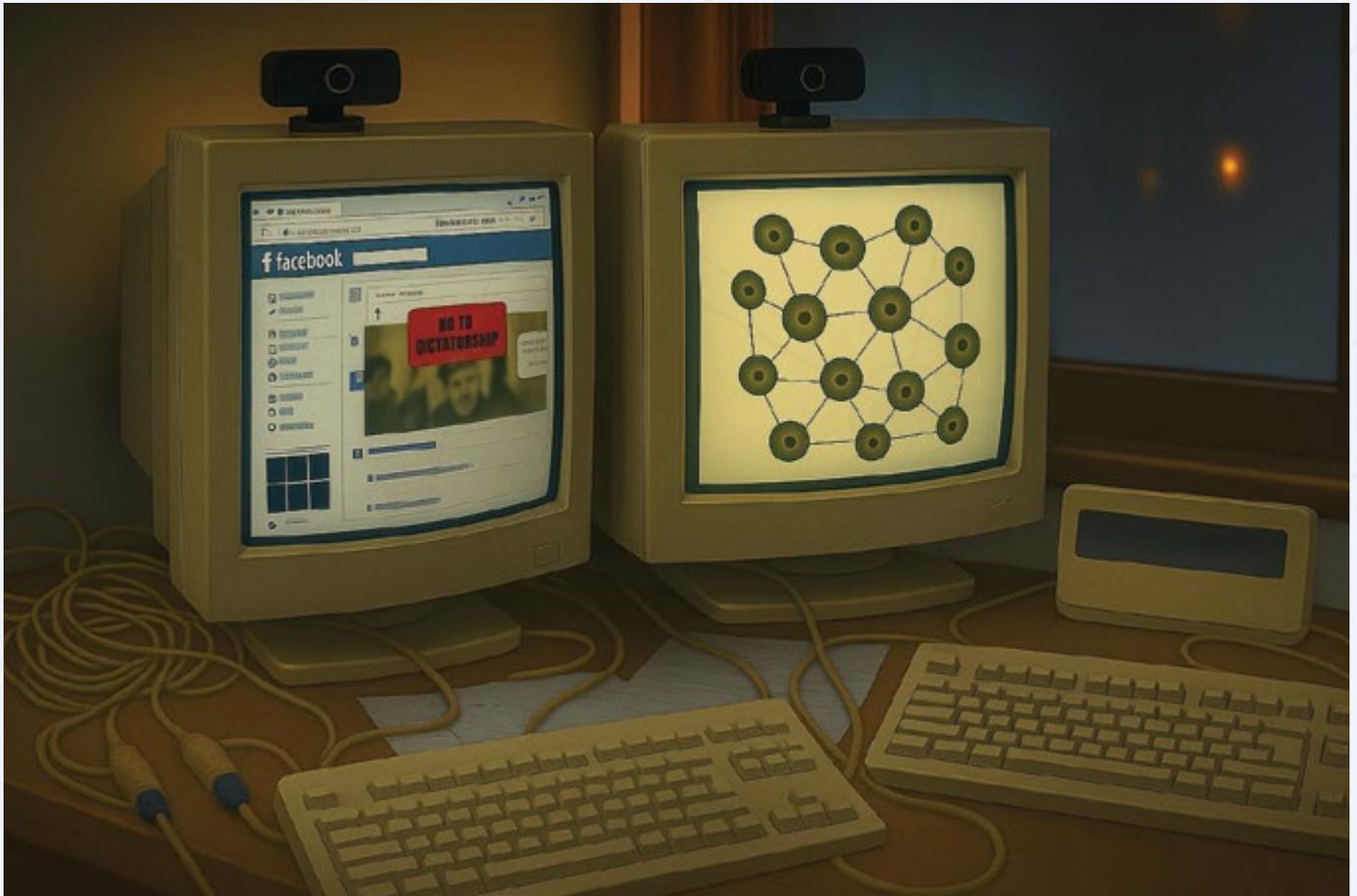
Finding community on social media

by KATHERINE FRANCISCO

From Friendster to Facebook, discreet blogs to divisive feeds, Katherine Francisco shares her emotional journey through the rise — and rupture — of digital communities. Set against the backdrop of Philippine politics, pandemic isolation and the lure of the endless scroll, she reflects on the double-edged sword of communication and connection via social media.

The year was 2006. I found myself sitting in front of a desktop computer, at the point of no return. Despite my extreme hesitation as a shy kid, I'd finally decided to sign up for Friendster, my first venture into social media.

It's not that I wanted to close myself off from the world. As a deeply insecure and easily embarrassed introvert, it just felt safer to play the part of the "smart, responsible kid" — serious, quiet, not the type to be silly and carefree.





But I had a killer sense of humour at home, and I wanted people to see that I could be fun too. I was always torn between the desire to be known and my fear of social judgement. The barrier Friendster provided between my self-expression and my physical self bridged these seemingly conflicting desires. Suddenly, there was balance — if I didn't have to deal with how I was being perceived in real time, I didn't have to worry about what I was posting online.

When I ventured into blogging, I began writing about things I wouldn't have had the courage to say in person: deep insecurities, existential problems, things I would later come to recognise as early indicators of depression. Friends would sometimes reach out and comment on my entries, but it often felt like I was writing for an audience of one, and there was freedom in laying my emotions bare without feeling exposed. It was also supplementing my real-life relationships: since there were lots of things about myself that I was only willing to express from behind the safety of a screen, only those who saw both my offline and online personas had access to the “real me”. It was like a cheat code; a way to deepen relationships without risking rejection and emotional hurt.

Over the years, I became aware of warnings about the dangers of social media — that algorithms were prioritising high-engagement content, that some of the posts had been covertly paid for to push certain agendas — but these comments felt like distant noise to me. As long as social media helped me manage my friendships, I didn't mind. If I could still enjoy the convenience of connecting with friends, then what did it matter if a feature had been altered or some terms of use changed? I was getting the feeling of community without having to put in the effort of in-person interactions. I didn't give much thought to all this until the 2016 Philippine national elections — and, later, the pandemic lockdowns — when suddenly both the tormentor and healer of my mental health existed in the same space.

My previous apathy meant I felt the shift in people's online behaviour as if everything had changed overnight. In the lead-up to the elections, it felt like everyone had to choose a side politically; nuance and shades of grey ceased to exist. We would later find out that this was partly the result of targeted propaganda created by the consulting firm Cambridge Analytica, who exploited the Philippines's high rate of online usage and relatively lax regulatory structures to use the country as a “petri dish” to — [in the words of whistleblower Christopher Wylie](#) — “experiment on tactics and techniques that you wouldn't be able to as easily in the West”¹.

It was like a cheat code; a way to deepen relationships without risking rejection and emotional hurt.

The most immediate effect was watching colleagues revealing where they stood on all manner of controversial political issues. I discovered, to my horror, that a kind lady in my office fully endorsed extrajudicial killings, and I watched as agreeable coworkers sharpened their metaphorical knives for battle online. I suddenly realised that I never knew what my ‘community’ truly looked like.

I understand, to some degree, why things were the way they were. Political parties were shaping their narratives around things that deeply resonate with Filipinos — discrimination based on ethnolinguistic identity, the struggles of the working class, resentment of the educated elite. Of course people were going to be emotionally attached to their political affiliations. This was clearly reflected in Facebook comments, where any criticism levelled at one's preferred politician was perceived as a personal attack.

Plenty of assumptions and generalisations were made; I was guilty of this too. I started painting people with a broad brush, based on where they came from. I knew that there were kind people out there, but it mattered little — if someone online referred to a particular region as their hometown, or displayed some sort of regional pride, my knee-jerk assumption of their character would almost always be negative. I started believing people to be hostile — even before I met them — because they finally felt seen, understood and represented by politicians whose ideals and morals I found questionable.

Avoidance seems to be a pattern for me when social situations get tough. The toxicity that spilled from the confines of the Internet into real life was something I could easily ignore by burying my head in the sand... at first. Then the pandemic hit, and there was no other way to seek community but go online.



Remove the genuine humanity of it all and we can see social media for what it really is: a mimicry of community, a space without soul.

It felt like navigating a labyrinth, with no guarantee of what would be around the next corner — I found relief in memes one moment, only to be devastated by news of mass deaths and Covid-19 deniers. I was stuck; as horrified as I was by what I saw on social media, turning away completely would have meant also turning away from comforting voices assuring me that we'd make it through these unprecedented times.

The realisation crept up on me that I'd willingly shot myself in the foot. By letting social media handle the emotional toll of building community for me, I'd dulled my ability to create or sustain connections without the crutch of messaging apps, memes and things that pinged on my phone. This became all the more difficult as personal struggles and family health issues led to a depression diagnosis in 2023. When you have a mental health disorder, seeking community support online gets doubly difficult; it's like a game of Russian roulette because you can never predict if you'll be greeted by compassion or hostility.

But there are still benefits to being on social media, as I learnt one sick day. Recovering from both a stomachache and an intense social media binge, I listened to *'It's Time to Stop Doom Scrolling'*, an episode of Chasing Life with Dr Sanjay Gupta, a podcast produced by CNN.² It was suggested in the podcast that one can reap the benefits of community through active engagement — posting and commenting — instead of passively lurking on pages. *Easier said than done*, I thought. How do you sincerely engage when the online community feels so very divided and spaces poisoned?

My desperation for some sort of connection did result in a silver lining: I found that smaller, moderated spaces felt like a return to something safer, something more reminiscent of the early days of social media. I began posting on the forums of Sanvello, a now-defunct app for mental health, banking on the assumption that surely no one in a tiny moderated forum would be a threat. It made me feel safe but also made me wonder if we'd really come to a point where the only safe spaces available online were moderated ones with community guidelines—as if we were all kindergarteners who needed to be told how to behave.

I know there'll always be bad actors online as long as there's money to be made. Still, I have hope when I see how genuine engagement, led by people who truly want to come together, can translate to real-world action. I saw hope in community pantries organised online during the pandemic by private individuals — first in one neighbourhood, then spreading to several places across the Philippines. I see hope in successful movements to boycott problematic companies as a show for solidarity with vulnerable populations affected by their activities. I see hope in online groups calling for volunteers, whether it be for pop idol concerts or political rallies. I have hope that this level of dedication to genuine causes will never be bought by money or corrupted by online bots.

It's frustrating to point to individual responsibility as a solution when the problem is actually systemic. But having an increased awareness of how we conduct ourselves online can be a starting point for real change, not only in social media spaces but also in our perception of what it truly means to build community. A deeper understanding of our own emotions and motives for engaging with content the way we do and a stronger desire for in-person connection can help strengthen our personal values. I've found that daily meditation helps me be more cognisant of my emotions and more easily break the spell of the endless scrolling that still negatively affects me.

The social media sphere has come so far since that moment in 2006 when I first joined the ranks of Friendster users. But the heart of it remains the same: humans, just wanting to be seen and to connect. Remove the genuine humanity of it all and we can see social media for what it really is, a mimicry of community, a space without soul. 

WRITER BIO:

Katherine Francisco is a communications professional with a degree in psychology from the Ateneo de Manila University. She likes keeping up to date with online pop culture and mental health topics. She lives in Manila with her family and a senior shih tzu dog, Charlie.

END NOTES

1. Exclusive: PH was Cambridge Analytica's 'petri dish' – whistle-blower Christopher Wylie. Paige Occeñola, *Rappler*, 10 September 2019. <https://www.rappler.com/technology/social-media/239606-cambridge-analytica-philippines-online-propaganda-christopher-wylie/>

2. Chasing Life with Dr Sanjay Gupta: It's Time to Stop Doom Scrolling. Dr Sanjay Gupta, *CNN*, 22 March 2022. <https://edition.cnn.com/audio/podcasts/chasing-life/episodes/a6e3342e-16de-411f-892d-ae5f013379ab>



Balance is an independent project.
We depend on support from our readers.

Support the BALANCE Fund
Your support helps us
keep this space alive.



Subscribe from
Now and 2026
Be part of what
comes next.



BALANCE AND GENERATIVE AI

At *Balance*, we approach Generative AI as both a powerful creative tool and a disruptive force with far-reaching implications for society, culture, and rights. We recognise its potential to expand creative possibilities, accelerate innovation, and enable new forms of storytelling and collaboration. At the same time, we remain deeply aware of its risks – including the reinforcement of bias, the spread of misinformation, the erosion of labour rights, and the concentration of power in the hands of a few corporations controlling its infrastructure.

Our use of Generative AI is intentional and transparent. We employ it where it adds value to the creative or editorial process, but always with human oversight and editorial judgment. We do not rely on AI to replace human voices, especially those from communities whose perspectives are already marginalised or underrepresented. Instead, we see it as one tool among many – one that must be critically examined, ethically deployed, and held accountable.

By openly engaging with Generative AI, we aim to explore its possibilities while questioning its impact. Through our coverage, collaborations, and creative work, *Balance* will continue to investigate who benefits, who is harmed, and how this technology can be shaped to serve the public interest rather than deepen existing inequalities.

FOR MORE INFORMATION, CONTACT US:
BALANCE@COMMONEDGE.ASIA

Resisting Oppression

Focusing on information needs

by PATRICK BOEHLER



People often look for information that guides them through daily life.

The traditional approach to fighting censorship can be an exhausting technical game. By focusing on a needs-first approach, Patrick Boehler discusses how the fight against censorship and oppression must provide information essential for daily life.

As a journalist, I've learnt about censorship resistance through failure. Years of working with international broadcasters have taught me that the news media excels at reaching people but fails at helping them. We measure success in audience numbers while communities struggle with immediate, solvable problems. Our content flew past censors and into irrelevance.

I worry we've created way too many unnecessary martyrs of journalism because we've never sufficiently questioned the premise of a lot of this work. I myself have asked and agonised over how to defeat censorship, assuming the relevance of everything my peers and I were producing. I should have been asking how to serve people's actual information needs.

Parents trying to find safe milk formula for their baby won't look up, and probably don't need, our investigative exposé on who's up-and-coming in politics or what was said at the last government press conference. What they need to know is which stores stock good, reliable products, which hospitals will treat their child without bribes, and which officials actually respond to complaints. This sort of mundane, actionable information threatens authoritarian control more deeply than any dissident broadcast.



The traditional approach to fighting censorship is an exhausting technical game. When governments block websites, we create mirrors. When they shut down platforms, we migrate our content. When they monitor communications, we adopt encryption. Meanwhile, the information and content we're protecting often serves our conception of importance more than actual community needs.

I've watched newsrooms invest millions in circumvention technology even as their audiences turn to WhatsApp groups for information that actually matters to them: which hospitals have vaccine stock, which neighbourhoods face demolition, which schools accept children without local registration. These informal networks lack sophisticated encryption but they solve real problems.

Across autocracies — and there's more and more of them around the world — communities already demonstrate this principle. They share real-time data about which employers actually pay wages, which local officials can be trusted, which schools accept migrant children. This information spreads through trusted networks, verified through lived experience rather than institutional authority, because they're actually important and necessary to people's lives.

Now we face AI systems that perfect authoritarian information control. When someone asks about rising food prices, AI chatbots provide soothing explanations about global supply chains while omitting local corruption. When people inquire about protests, they're given "historical context" about the importance of stability. The censorship is becoming conversational, personalised, invisible.

These systems excel at providing general information while systematically obscuring actionable details. They'll provide comprehensive explanations about labour law but can't tell you about the reputation, work ethic and interpersonal manners of lawyers who take on such cases. They'll discuss the importance of environmental protection while avoiding mention of specific local sources of pollution.

A needs-first approach reveals how censorship actually works. Authoritarian systems don't just block information — they create environments where people can't act on what they know. It's not enough to understand your rights; you also need to know which lawyers will be able to help you assert them. Documenting pollution only matters if you know who will actually investigate.

Communities navigating these restrictions become laboratories for information efficiency. They teach us that relevance trumps reach, that trust grows through service, and that the most powerful networks emerge from shared needs rather than shared ideology. When we start with community needs, unexpected allies emerge. The grandmother sharing pension information doesn't see herself as a resistance fighter. The parent documenting school corruption doesn't identify as an activist. Yet their actions, multiplied across neighbourhoods, create information flows that autocrats struggle to control. It's harder to criminalise sharing hospital ratings than organising protests.

Networks built on meeting real needs create their own momentum. People invest time and risk in systems that demonstrably improve their lives. Communities that successfully share medicine prices develop verification habits. Families trading school information build secure communication practices in the

face of efforts to stop or threaten them. The infrastructure for sensitive information grows from mundane utility.

This approach also changes how we think about sustainability. We don't need to fund grand institutions that become hollow vessels for whoever controls the next funding cycle. Small networks solving immediate problems resist capture better than any bureau or initiative.

As AI systems become primary information interfaces, this community-based approach becomes essential for preserving truth. When every parent in a district knows through direct experience which schools accept migrant children, no algorithm can maintain convenient fictions. Lived experience shared through trusted networks defeats even sophisticated computational propaganda.

The path forward starts with inverting our assumptions. Begin with needs, not messages. Build networks that solve problems, not platforms that broadcast positions. The most subversive act might be helping people find good schools. The most revolutionary technology might be accurately tracking which hospitals have clean blood supplies.

Providing information so essential to daily life that restricting it becomes impossible — that's how communities protect truth in an age of algorithmic mediation. Not through technical cleverness or institutional grandeur but through the simple act of neighbours helping each other navigate the world as it actually is. 

WRITER BIO:

Patrick Boehler is based in Brooklyn and leads Gazzetta, a media research lab helping newsrooms serve communities in restrictive environments. After years as a reporter and editor in international journalism, he now focuses on making media genuinely useful rather than merely accessible.



The Mix: Highlights, insights, and diversions

A first-of-its-kind global survey reveals the frightening reality of land and environmental defenders on digital spaces

Social media platforms and online spaces can be a powerful tool for community mobilisation and awareness raising, but they also have a business model reliant on the attention economy where manipulative disinformation and rage bait get more clicks. Defenders who are often the planet's last line of defence face the brunt of this business model, especially as big names like Meta and X are making changes to their operations that could actively reduce protections offered to users.

READ GLOBAL WITNESS' LATEST FINDINGS HERE



As platforms actively bankroll harmful activity online, information integrity and democracy are being pushed to the backburner

The rise of social media monetisation, the proliferation of inauthentic automation, and the redefinition of advertising models and publisher relationships are giving rise to dangerous tactics on social media. Playing under these new rules, authentic content creators can't compete with automated fake accounts mass producing and distributing content that's increasingly harder to attribute.

READ WHAT TO FIX'S POLICY BRIEF ON THE EVER-EVOLVING CHALLENGES OF REINING IN BIG TECH HERE



'Anything you put online can [be] and probably has been scraped'

Researchers audited just 0.1% of a major AI training set to find thousands of images, including identifiable faces and identity documents. The real number could be in the hundreds of millions, showing that nothing online is safe. As William Agnew, a postdoctoral fellow on AI ethics puts it, "anything you put online can [be] and probably has been scraped".

READ ABOUT THE STUDY HERE



Israel's terrifying AI-backed panopticon in Gaza

Israel is testing the latest forms of surveillance and killing in Gaza, including by building a huge database on every Palestinian under occupation. With human life becoming mere data points for powerful states to do with as they wish, Gaza exposes the brutality of futuristic technology.

READ ABOUT ISRAEL'S FRIGHTENING USE OF AI IN GAZA HERE



New technologies bring new battlefronts to Indian education institutions

Indian educational institutions are rapidly adopting new technologies, but falling behind on cybersecurity. This has left them vulnerable to a wide range of cyberattacks – some of which are also targeting students.

READ ABOUT CYBER-PEACE FOUNDATION'S REPORT HERE.



AI agents vulnerable to hijacking attacks

Popular AI agents and assistants from major companies like Google and Open AI are susceptible to being hijacked with little or no user interaction. Research shows how hackers could exfiltrate data, manipulate critical workflows across targeted organisations and, in some cases, even impersonate users. Beyond infiltrating these agents, attackers could also gain memory persistence, allowing them to maintain long-term access and control.

READ ABOUT ZENITY
LABS' FINDINGS HERE



TikTok's reckoning with the 'real' world

TikTok leaves little to the imagination – if you wish to see something, you can find it on the short video app. Opening doors to the lives of people around the world, TikTok makes us all voyeurs in a way that other social media apps are yet to master. One reason for this is its “undiluted reality checks”, says J. Wortham as he explores the live streaming of manual labour on the app.

READ THE FULL
ARTICLE HERE



China's thriving Automated Vehicles (AVs) industry

More self-driving cars are tested there than anywhere else in the world. By 2030, a fifth of new cars sold in China will be fully driverless, and 70% will feature advanced assisted-driving technology, according to the China Society of Automotive Engineers.

READ ABOUT THE
STUDY HERE



An AI doctor and bromide toxicity

After reading about the negative effects of table salt, a man consulted ChatGPT about eliminating chloride from his diet and started taking sodium bromide over a three-month period. Soon he developed a rare condition – bromism, also known as bromide toxicity.

READ THE ANNALS OF
INTERNAL MEDICINE
CASE REPORT HERE.



Doodles in your electronics

Silicon doodles were used by designers in the old days of technology as a form of expression and to protect against technological theft. The doodles – from tame like their initials to whimsical like a dinosaur driving a car – are a rarity today. But they remain a gentle reminder of the human behind the machine, and a group of collectors are racing against time to document them.

READ THE NEW YORK
TIMES' REPORT HERE

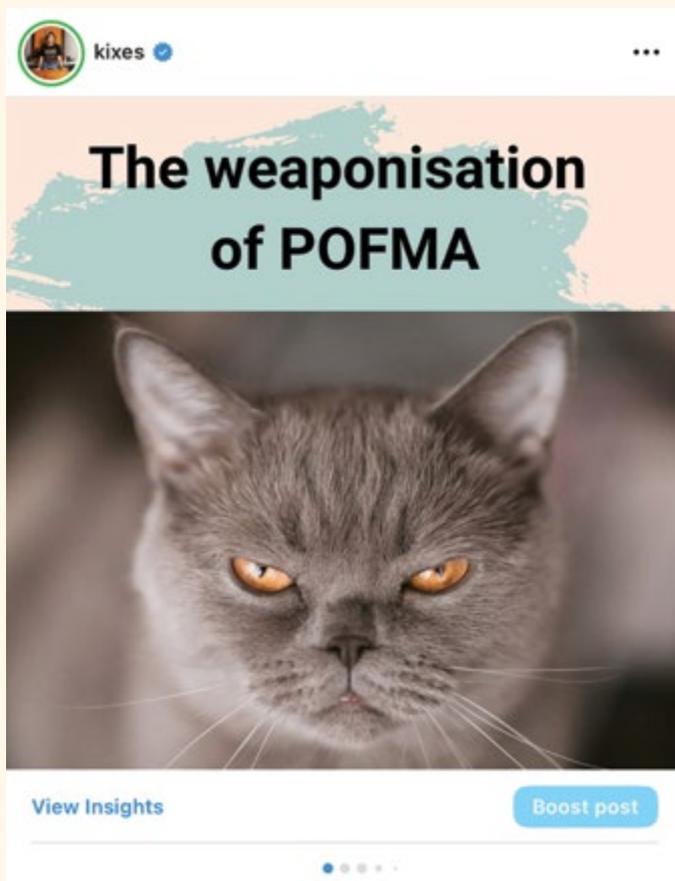


Networks and Minefields

When social media presents both opportunity and risk

by KIRSTEN HAN

In the early days, social media networks were viewed optimistically as democratising tools: they gave ordinary folk the means of circumventing state censorship and suppression to communicate directly with one another. The intervening years have disabused us of this notion, revealing social media as yet another fraught site of contestation and control. Kirsten Han reflects on her experience as an activist in Singapore and civil society's relationship with social media platforms in a difficult political environment.



Social media has been key to Singaporean activism efforts.

I'm sitting at the registration booth for the Transformative Justice Collective's (TJC) event, trying to look welcoming and approachable, when three young volunteers come up to me. "Sorry, Kirsten, can we use this space? We need to make a TikTok video."

I make myself scarce; our event is winding up anyway. By the time I get home a few hours later, the video they shot promoting TJC's merchandise—which we sell to try to recoup the cost of our events—is already getting likes and shares on TikTok and Instagram Reels.

This is how civil society activism functions in Singapore in 2025. In-person events are great if you can navigate the legal and logistical minefield: overly broad legislation that restrict freedom of assembly, authorities that pop up at any time insisting that licences or permits are required for the most trivial of things, venues that might balk at the idea of hosting an event perceived as "politically sensitive" or "controversial", venues that don't balk at the idea but have to charge hefty rates to keep their own business afloat in expensive city. But social media is indispensable.



I often come across people—even some who have lived, or still live, in Singapore—who are under the impression that there’s no activism in my country. They assume that, because Singapore has a reputation of being a restrictive one-party state, the government’s control is so total that there’s almost no dissent on the ground. But while it’s true that Singapore is an authoritarian state where civil liberties are suppressed, there’s plenty of civil society activity. You just need to know where to look. And the place to look is online.

Space for expression is heavily restricted in Singapore. Public assemblies for a cause—as determined by the authorities in arbitrary fashion—are criminalised unless a prior permission has been obtained from the police. The expansiveness of this law has led to police investigations, and sometimes even criminal charges, into actions ranging from [a single person holding a smiley face drawn on a piece of cardboard](#)¹ to [a group of Singaporeans delivering letters to the Prime Minister’s Office](#).² There’s only a single park in the entire country where demonstrations can be held without having to first apply for a police permit, and even this space is still subject to other regulations, such as a ban on foreigners participating and restrictions on events that touch on issues of race and religion.

The mainstream media can’t be counted on, either. Two major companies control the bulk of Singapore’s traditional media outlets; both have close ties to the government and are known to largely toe the establishment line. Critical voices and stories aren’t given much space—if any—in local broadsheets or TV news.

In such a political environment, Singaporeans can only rely on our own efforts to generate public discourse on important issues that the state would rather obscure.

I’m an activist child of the Facebook era. My involvement in Singaporean civil society began in 2010, a time when the social media network was making its presence felt in Singaporean politics. After decades of gate-keeping and censorship by state agencies and the mainstream media, Singaporeans suddenly had a space where we could disseminate information, engage in discussion and promote events—without interference and at scale. I volunteered at *The Online Citizen*, a citizen journalism website that promoted our original reporting and commentaries on Facebook. I started my own blog on the side.

When the 2011 general election came around and opposition parties realised that they could finally circumvent biased media reporting and directly address voters, many of us were optimistic about social media’s potential to be a total game-changer in the push for true democracy in Singapore. The election that year saw the lowest vote-share for the ruling People’s Action Party since independence, and a team from an opposition party won a mega-constituency (known in Singapore as a Group Representation Constituency, or GRC) for the first time.

Looking back now, we were hopelessly naïve. The assumption that social media platforms would always be the domain of independent and dissenting views was, in today’s chronically online Gen Z parlance, “delulu”. The ruling party might have been caught on the back foot in 2011, but once they realised the potential of social media it was only a matter of time before they started dominating the game, as they’ve done with every space in Singapore. They are, after all, the ones with the ability and resources to make laws and regulations, to police and suppress, and to pay top dollar for polished online campaigns.

Today, social media platforms—no longer just Facebook but also others like Instagram and TikTok—are fraught spaces of contestation, surveillance and control. Singaporean activists—especially those working on issues related to Palestine, sexual violence, labour rights or capital punishment—fret over being shadow-banned, a practice in which social media algorithms down-rank, delist or even block content without any transparency. And we know that the government is keeping a close eye on our social media content, ready to pounce on any (real or perceived) weakness.

In Singapore, activism persists—not on the streets or in headlines, but in Telegram groups, TikTok posts and WhatsApp broadcasts shared quietly and deliberately.



We can't afford to quit social media, even if it's hostile territory. For activists, it remains the fastest route to connection, mobilisation and public discourse.

TJC has received multiple executive orders from the government under the Protection from Online Falsehoods and Manipulation Act (POFMA), accusing us of spreading “fake news”. Last December, our website and social media pages across Facebook, Instagram, X (previously Twitter) and TikTok were designated “declared online locations” under POFMA, introducing such onerous restrictions and conditions — for example, banning us from deriving “material benefit” for the online work we did on those platforms, requiring us to undertake the impossible task of trying to completely separate our offline and online activities — that we decided to [stop operating those pages](#) for the duration of the two-year designation.³ On top of that, the collective, and three of its members, are subject to criminal investigations under POFMA—if charged and convicted, the penalties could involve heavy fines or even jail time.

Social media can also be weaponised by powerful politicians to direct harassment—coordinated or otherwise—against their critics. I’ve experienced this myself: a politician publishes a Facebook post full of insinuations and dog-whistles, and the next thing you know, you’re drowning under a torrent of condemnation and insults. Any clarification or rebuttal issued might reach some people but will generally be drowned out by the state’s much larger megaphone on both social media and traditional news outlets. This isn’t just harmful to the target; it’s also a warning to others, a demonstration of the cost of dissent. No one wants to attract this sort of attention from a government minister.

Still, calls to “delete Facebook” and get off social media fall flat in Singapore. It’s just not an option, especially for those of us who have messages to get out there and ideas to communicate. We might be repulsed by the big tech companies’ willingness to cosy up to authoritarians and be highly sceptical of social media algorithms, but we ultimately still need these platforms because there aren’t many other options in this political environment. Social media is still the easiest, most low-cost way for under-resourced activist groups to reach a maximum number of people in a short amount of time. And it does still work: I’ve been repeatedly told by strangers I meet at TJC events that they learnt about our work and activities through Instagram.

The trick, then, is to maximise the use of social media platforms but not be held hostage by the whims of their algorithms. In choosing to temporarily ditch our “declared online location” pages, TJC has pivoted

to mailing lists and broadcast channels on WhatsApp and Telegram—much more direct channels of digital communication that could potentially work out better in the long run. And as people tire of the petty fights and AI slop taking over their social media feeds, there’s been a resurgent growth in appreciation for more intimate in-person interactions. We’re rediscovering the beauty of small-scale workshops, of “underground” organising and quality time spent with friends and comrades talking about shared struggles.

Activism is, at the end of the day, all about connection: between struggles, between communities, between people. Social media has been key to Singaporean activism efforts and that looks set to continue even if online spaces are not longer as safe as they once were. But we no longer live under the illusion of it being the most promising path to a better future.

WRITER BIO:

Kirsten Han is a Singaporean writer, editor and activist. She runs We, The Citizens, a newsletter covering Singapore from a rights-based perspective, and is a member of the Transformative Justice Collective, where she works for an end to the death penalty and the war on drugs. She’s also an executive committee member of NIMBUS, a network of solidarity among Singaporean groups engaging in acts of journalism and media-related work, and the managing editor of Mekong Review, an Asia-focused literary journal.

END NOTES

1. Singapore: Jolovan Wham charged for holding up a smiley face sign. Presto Jha, BBC News, 27 November 2020. <https://www.bbc.com/news/world-asia-55068007>
2. Trial begins for 3 women charged over pro-Palestinian ‘procession’ to Istana. Koh Wan Ting, CNA, 1 July 2025. <https://www.channelnewsasia.com/singapore/three-women-organise-procession-istana-claim-trial-court-5214001>
3. NOTICE: TJC ceases operations of our website and social media accounts till December 2026. Transformative Justice Collective, 21 January 2025. <https://transformativejusticecollective.org/2025/01/21/notice-tjc-ceases-operations-of-our-website-and-social-media-accounts-till-december-2026/>



EVENTS & CONFERENCES

2025 GLOBAL GATHERING – DIGITAL RIGHTS DEFENDERS

LOCATION: ESTORIL, PORTUGAL

Dates: September 8–10, 2025

A three-day in-person gathering where digital rights defenders, civil society actors, and journalists converge to collaborate on critical technology-related challenges impacting human rights. A key forum for networking, strategy-building, and cross-border solidarity in defense of digital freedoms and civic rights.

<https://gathering.digitalrights.community>

TOKEN2049 ASIA – SINGAPORE

LOCATION: MARINA BAY SANDS, SINGAPORE

Dates: October 1–2, 2025

TOKEN2049 is the world's largest crypto and blockchain event, bringing together over 25,000 attendees, 7,000 companies, and 300+ speakers across five immersive floors—conference stages, exhibition halls, entertainment zones, wellness areas, live DJs—in one of Asia's most iconic venues.

<https://www.asia.token2049.com>

NETWORK STATE CONFERENCE

LOCATION: SINGAPORE

Date: October 3, 2025

This event brings together visionaries interested in founding, funding, and building new communities, featuring speakers like Vitalik Buterin, Amjad Masad, Nuseir Yassin, as well as representatives from Solana and Coinbase. A fit for anyone exploring digital societies and internet-first institutions.

<https://ns.com/conference>

SPLICE BETA 2025

LOCATION: CHIANG MAI, THAILAND

Dates: November 17–18, 2025

Splice Beta is a dynamic media-startup festival designed for journalists, creators, founders, and media innovators. It offers a welcoming, inclusive environment to build viable media businesses through workshops, coaching, mentorship, and community.

<https://splicemedia.com>

GLOBAL INVESTIGATIVE JOURNALISM CONFERENCE (GIJC25)

LOCATION: KUALA LUMPUR, MALAYSIA

Dates: November 20–24, 2025

GIJC25 is the world's largest international gathering of investigative journalists. Hosted for the first time in Asia, the event features cutting-edge workshops, training sessions, and networking opportunities at the Kuala Lumpur Convention Centre to foster collaboration across borders.

<https://gijc2025.org>

AI SUMMIT DELHI (INDIAAI IMPACT SUMMIT)

LOCATION: NEW DELHI, INDIA

Date: TBD, expected February 2026

The IndiaAI Impact Summit (AI Summit Delhi) is a major gathering shaping the future of equitable and responsible AI. Organized by IndiaAI, the summit convenes government, industry, and academic stakeholders to explore international cooperation in AI for societal impact.

URL: <https://impact.indiaai.gov.in/home>

2025 DIGITAL RIGHTS AND INCLUSION FORUM (DRIF25)

LOCATION: LUSAKA, ZAMBIA

Dates: April 29–May 1, 2025

DRIF25 convenes stakeholders from the Global South to safeguard the internet as a civic space. This forum emphasizes digital inclusion, civic participation, and protecting online freedoms—particularly crucial for communities facing shrinking digital spaces.

URL: (Search for "Digital Rights and Inclusion Forum 2025") UN Global Compact Network Australia+6drif.paradigmhq.org+6conferenceindex.org+6 (Note: direct URL not listed in search results; you can locate via official DRIF or Paradigm Initiative channels.)

RIGHTSCON 2026

LOCATION: LUSAKA, ZAMBIA (AND ONLINE)

Dates: May 5–8, 2026

RightsCon is the leading summit on digital rights, bringing together activists, policymakers, technologists, and journalists. In 2026, the conference returns to Africa—its first-ever in Southern Africa—with both in-person and virtual programming.

<https://www.rightscon.org>

IF YOU WANT TO SHARE YOUR EVENTS, CONFERENCES - BIG OR SMALL - WITH US,
PLEASE EMAIL balance@commonedge.asia

False Starts and Stalled Reforms

Australia's tech regulation landscape

by LIZZIE O'SHEA

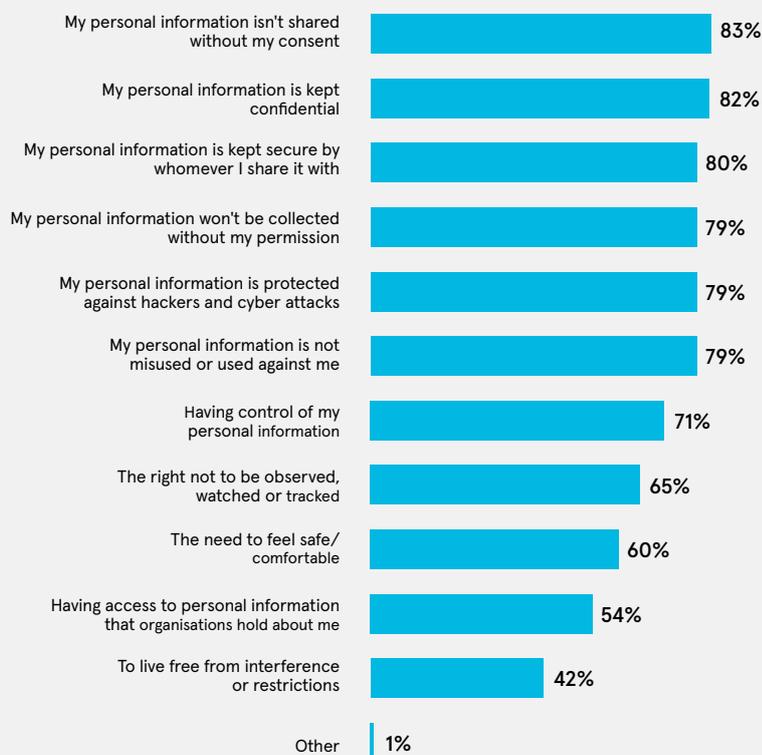
Lizzie O'Shea explores Australia's uneven approach to tech regulation, highlighting the gap between public support for stronger safeguards and a political system swayed by industry influence and the global power of Big Tech.

Amid the chaos and cruelty of the second Donald Trump administration in the US, the interests of Big Tech have aligned with state power in ominous ways. It's a situation that's forced many digital rights activists to rewrite their strategies. Any potential regulation of technology comes with an appreciable risk of generating a diplomatic confrontation with the US (to the extent that a tariff war can be described as diplomacy). Many countries — especially those that have been allies of the US since the end of the Second World War — are contending with the meaning of sovereignty in a world that's technologically connected, with giant US companies operating at all levels of the stack. For reasons both understandable and unforgivable, many regulators are opting for stasis over leadership.

In recent years, Australia has developed a reputation for regulating Big Tech in ways that are being emulated in other parts of the world. Australia was the first country in the world to establish [an agency](#) committed to keeping its citizens safer online.¹ It was the place that created the [news media bargaining code](#),² facilitating payments from digital platforms to media organisations — a model later also adopted in Canada and New Zealand. Most recently, Australia introduced [a social media ban](#), described as another world first, for children under sixteen years of age.³

They may look like bold moves, but these regulatory initiatives are not without their failings. The eSafety Commission is overseeing [the development of online codes of practice](#) that have seen increased dependence on automated decision-making for content moderation, age assurance technology and privacy invasive design.⁴ The news media bargaining code has been criticised for failing to secure funding for public interest journalism,

What Privacy Means to Australians



SOURCE: WWW.OAIC.GOV.AU

Findings from the Australian Community Attitudes to Privacy Survey Survey 2023, conducted by the Office of the Australian Information Commissioner.



with [the real winners being large media companies](#) like Rupert Murdoch’s News Ltd.⁵ (In Canada, the equivalent initiative has been [labelled a fiasco](#).⁶) Meanwhile, the social media ban is facing genuine — and anticipated — [operational challenges](#).⁷ The proposal has been significantly controversial for a variety of reasons, even [attracting criticism from those administering it](#).⁸

There’s something commendable about Australia’s regulatory zeal, but it’s telling how poorly it is often directed. Privacy reform, which the current government has been accepted as a necessity, remains stalled. It’s increasingly clear that the tech industry, sensing an opportunity, is leaning hard into [productivity arguments against privacy reform](#) — mainly in service of allowing AI to develop unimpeded.⁹ In a [recent submission](#), Meta said it was “concerned that recent developments are moving Australia’s privacy regime to be out of step with international norms ... and [will] disincentivise industry investment in AI in Australia or in pro-consumer outcomes.”¹⁰ Strong privacy reform has the potential to improve the online experiences of people of all ages, but powerful and well-resourced opponents are successfully diverting the conversation and delaying regulatory action.

This sits in sharp relief to public opinion. Australians have consistently polled as strongly supportive of improved privacy protections.¹¹ Almost all Australians think they should have additional rights under the Australian Privacy Act. Nine in ten Australians want the government to provide more legislation that promotes and protects the privacy of individuals. The Australian government’s neglect of this issue belies a reform agenda that’s shaped less by bravery and more by the banality of politics and vested interests.

The public also has strong views on AI, the other field of tech regulation which has moved at a laggardly pace. The Australian government has introduced a voluntary safety standard but no enforceable regulation. Australia ranks among the lowest globally on acceptance, excitement and optimism about AI — only 30% of Australians believe the benefits of AI outweigh the risks.¹² This has largely been understood as a problem of attitude rather than an issue of power or politics. But Australians are more sensible than that: 77% agree regulation is necessary and 83% say they would be more willing to trust AI systems when assurances are in place. Rather than inhibiting the embrace and adoption of AI technology, strong regulation would do the opposite.

In some ways, therefore, the job of digital rights activists is straightforward: remind elected leaders who they work for. We must speak for the majority of everyday people who want strong privacy reform and AI regulation. We need to ask questions about who benefits from failing to act on these issues, or acting in ways that are ineffective and inept. During this Trump administration, representative democracy is facing increased pressure and fault lines are emerging. Tech policy is one such example, in and Australia’s experience demonstrates that — if not properly consultative or thoughtful — both action *and* inaction in the face of growing tech power can lead to a government failing its citizens. 🇺🇸

WRITER BIO:

Lizzie O’Shea is a founder and the chair of Digital Rights Watch, which advocates for freedom, fairness and fundamental rights in the digital age. She also sits on the board of Blueprint for Free Speech. She speaks regularly about law, technology, and human rights, and her writing has appeared in the New York Times, Guardian, and Sydney Morning Herald, among others.

END NOTES

1. **What we do.** eSafety Commissioner. <https://www.esafety.gov.au/about-us/what-we-do>
2. **News media bargaining code.** Australian Competition & Consumer Commission. <https://www.accc.gov.au/by-industry/digital-platforms-and-services/news-media-bargaining-code/news-media-bargaining-code/>
3. **Swimming between the digital flags: helping young Australians navigate social media’s dangerous currents.** Julie Inman Grant, eSafety Commissioner, 24 June 2025. <https://www.esafety.gov.au/newsroom/blogs/swimming-between-the-digital-flags-helping-young-australians-navigate-social-medias-dangerous-currents>
4. **Australia is quietly introducing ‘unprecedented’ age checks for search engines like Google.** Ange Lavoipierre, ABC News, 11 July 2025. <https://www.abc.net.au/news/2025-07-11/age-verification-search-engines/105516256>
5. **Do bargaining codes have a future?** Public Media Alliance, 8 April 2024. <https://www.publicmediaalliance.org/do-bargaining-codes-have-a-future/>
6. **Canada’s law to help news outlets is harming them instead.** The Economist, 16 May 2024. <https://www.economist.com/leaders/2024/05/16/canadas-law-to-help-news-outlets-is-harming-them-instead>
7. **Technology to enforce teen social media ban is ‘effective’, trial says. But this is at odds with other evidence.** Lisa M. Given, The Conversation, 20 June 2025. <https://theconversation.com/technology-to-enforce-teen-social-media-ban-is-effective-trial-says-but-this-is-at-odds-with-other-evidence-259373>
8. See note 3.
9. **Meta argues its AI needs personal information from social media posts to learn ‘Australian concepts’.** Josh Taylor, The Guardian, 17 July 2025. <https://www.theguardian.com/australia-news/2025/jul/17/meta-ai-facebook-instagram-personal-information-social-media-posts-learn-australian-concepts>
10. **Cut privacy red tape to boost innovation: tech giants.** Tess Ikononou, In Daily, 17 July 2025. <https://www.indailyqld.com.au/news/just-in/2025/07/17/cut-privacy-red-tape-to-boost-innovation-tech-giants>
11. **Australian Community Attitudes to Privacy Survey 2023.** Office of the Australian Information Commissioner, 2023. <https://www.oaic.gov.au/engage-with-us/research-and-training-resources/research/australian-community-attitudes-to-privacy-survey/australian-community-attitudes-to-privacy-survey-2023>
12. **Global study reveals Australia lags in trust of AI despite growing use.** KPMG, 29 April 2025. <https://kpmg.com/au/en/home/media/press-releases/2025/04/global-study-reveals-australia-lags-in-trust-of-ai-despite-growing-use.html>



As easy as ordering dinner tonight



BUY. GIFT. OWN.

JOURNALISM IMPACT

Sown by **courageous reporters**
Scored with **AI**
Stored on **blockchain**

*For every \$1 given, you
power impact worth:*

Story leads to women gaining
access to temple after 400 years

\$14.1



Investigative report returns human
trafficking victim back to her family

\$19.6



Teacher suspended after exposé on
food stealing scam

\$8.1



CHECKOUT



VoiceDeck

*Where citizens fund concrete
journalism outcomes.*

<https://app.voicedeck.org/>



Power Plays

The uncomfortable position between governments and tech companies

by SARITHA IRUGALBANDARA

While government regulations often claim to be about protecting people from online harms, advocates and activists are well aware of how such legislation and rules can be used to oppress and expand authoritarian control. On the other end, the major technology companies of the Global North have consistently prioritised their bottom lines over genuine desires to ensure online safety for their users. Saritha Irugalbandara reflects on how civil society, caught between these two overwhelming players, needs to proceed with determination and thoughtfulness.

A year and a half since its dramatic entrance into Sri Lanka's legal ecosystem, the Online Safety Act (OSA) remains a political hot potato. Although the OSA originated from the Ministry of Public Security, the Ministry of Mass Media is now looking to [make amendments to the law](#).¹ This renewed discussion is also accompanied by Sri Lanka's ambitions for expanding digital public infrastructure and economy.



IMAGE CREDIT: SRI LANKA: ONLINE SAFETY ACT MAJOR BLOW TO FREEDOM OF EXPRESSION - AMNESTY INTERNATIONAL

Amnesty International describes Sri Lanka's Online Safety Act as a 'major blow to freedom of expression'.

Since it was rushed through the legislative process in 2023, the OSA has been one of the most controversial laws introduced by the previous administration led by Ranil Wickremesinghe. Amnesty International slammed it as a [“major blow to freedom of expression”](#).² Others have criticised it on the basis of serious implications for privacy, pointing to how this could [harm already marginalised groups](#) like the country’s LGBTQ+ community.³

The OSA was indubitably a response to the 2022 people’s movement that had been largely mobilised through social media and private messaging platforms. The mass protests against the government led to the eventual resignation of President Gotabaya Rajapaksa, who temporarily fled the country. Within days of being appointed the caretaker president, Ranil Wickremesinghe — who had previously been the prime minister — made it his first order of business to [brutally disperse protesters](#) occupying Galle Face Green, a park in the heart of Colombo. His second order of business: announcing that measures were underway to [introduce a law to regulate social media](#), drawing inspiration from regulations in Singapore.

The [role of Facebook](#) in the 2018 Digana anti-Muslim riots — during which two people were killed and hundreds of Muslim-owned homes and businesses were attacked — was a watershed moment that snowballed into a vibrant and diverse movement of digital rights activists, legal experts, researchers, policy analysts, journalists, academics, trade unions and think-tanks in Sri Lanka. Although this movement failed to prevent the passage of the OSA years later, it managed to exert enough pressure to compel the government to [reconsider the law’s implementation](#) in its current form.⁴ Civil society continues to grapple with the convergence of state and corporate tech power, and Sri Lanka presents an important litmus test for the Global South’s ability to resist regulatory capture while confronting what experts in South Asia call [the “contagion effect”](#), referring to situations in which “emerging markets in South Asia are implicitly compelled to adopt governance frameworks and regulations set by dominant markets, primarily in Australia, Canada, the European Union (EU), and the United States”.⁵

The power dynamic between Big Tech and the Global South has always been uneven; a relationship sustained by empty platitudes from the former and polite smiles from the latter.

The lack of transparency from Big Tech on their actual moderation practices is a global issue. By [downsizing their trust and safety teams](#), leaving the moderation of content in non-English languages [largely under-resourced](#), and blowing hot-and-cold when engaging civil society, the tech companies have by and large failed to build trust — especially in the Global South — in their commitment to even the most basic safety standards.⁶ However, there are rare moments when the interests or concerns of civil society and Big Tech appear to align, creating opportunities for civil society lobbying.

This was seen when the Asia Internet Coalition (AIC) — an industry association focused on internet policy in the Asia-Pacific region, with companies like Meta, Google, Apple and Amazon among its members — released a [statement](#) within ten days of the gazetting of the Online Safety Bill in 2023, expressing concern at the lack of stakeholder consultations and the law’s potential to “dampen innovation by restricting public debate and the exchange of ideas that can consequently impact the digital economy”.⁷ A lengthier [policy submission](#) followed in December that year, pointing to concerns that “overbroad and vague definitions of terms such as ‘facts,’ ‘false statements,’ and ‘feelings of ill-will’ also raise the concern for significant abuse, misunderstanding and threats to users’ ability to access and use information and knowledge”. Big Tech’s corporate interests were more clear in other parts of the policy submission: another key concern raised was the need for “safe harbour” provisions that reduce liability thresholds for companies for harmful content published on their platforms.



Anti-tech nationalism has been replaced with the more attractive e-nationalism: unique digital IDs, data monopolisation and centralisation.

According to a newspaper owned by the then-Public Security Minister, a meeting between the ministry and “civil society and media reps” [took place in October 2023](#). But many civil society actors who’d been working on the issue hadn’t been invited; participants had been selected through backchannel communications. The ministry later also [met the AIC in Singapore](#), but the outcome of these consultations have never been publicly divulged by the ministry, the AIC or other parties. When the amendments were tabled, many in civil society pointed out that no substantive changes had been made in relation to concerns about freedom of expression and privacy. Instead, the amendments focused on [reducing the liability of technology companies](#). There had been no genuine, meaningful consultations, but many of us expected this from a government that had already demonstrated its authoritarian tendencies and its lack of interest in fostering goodwill with civil society.

This experience with the OSA reminds me of another instance in which the AIC had been involved in tech regulation in Sri Lanka. In 2022, the AIC represented Big Tech in providing input on [SAFEWebLK](#), a Sri Lankan initiative to develop a voluntary code of practice akin to New Zealand’s Code of Practice for Online Safety and Harm. SAFEWebLK was positioned as the first attempt in Asia to create such a code and was meant to be the product of a collaborative process involving the tech industry, civil society, mass media, government and academia. To make it relevant to the local context, a series of public consultations were held to gather insight into the online safety issues that needed to be prioritised. It all seemed promising at the time: the draft and review processes were led by a team of diverse experts, public consultations included many different communities and identities, and industry engagement, through AIC, seemed forthcoming.

Promise can help build, but it can also blind. Within months of its launch in 2022, New Zealand’s Code of Practice for Online Safety and Harm was being scrutinised by the country’s government and civil society. Some [criticised](#) it for being a fig leaf for Big Tech’s attempts to pre-empt and deflect strong regulation. Concerns about the code being an industry-led effort to subvert New Zealand’s institutions and online safety mechanisms began to surface. These critiques should have been a warning for us in Sri Lanka; ultimately, the tech industry unilaterally decided that SAFEWebLK was not worth pursuing beyond a third iteration and abandoned it in early 2023. Whether this decision came from a lack of faith in a Global South country’s ability to implement a voluntary code, or perhaps because a more lucrative opportunity had come up for these companies, is worth a post-mortem.

The power dynamic between Big Tech and the Global South has always been uneven; a relationship sustained by empty platitudes from the former and polite smiles from the latter. As someone involved in the final months of active work on SAFEWebLK, I wonder, two years later, whether it’s even possible for the Global South to engage in a truly consultative process with Big Tech to produce mutually beneficial frameworks. Such processes require good faith and a working relationship premised on common values. What could under-resourced “small markets” possibly have in common with trillion-dollar companies wielding unprecedented power, resources, and influence?

Where New Zealand’s code of practice might have been a fig leaf, SAFEWebLK may have unfortunately paved a road to greater gains for the tech industry with the draconian OSA — with little market power or political leverage to actually hold companies liable, the full weight of the state’s authoritarian tendencies can be aimed strictly at its population with greater ease. Although the AIC did adopt some of the same language as rights-focused advocates in communicating issues at the early stages of the OSA, we cannot make the mistake of assuming that such trade lobbies will do any more than what they were created for. Their terms of engagement are bound to prioritise their bottom lines: reducing intermediary liabilities, pushing for safe harbour guarantees, and ensuring that their consumer bases aren’t threatened.



This is not to fault Sri Lankan civil society for engaging with the AIC on either SAFEWebLK or the OSA, or even to caution against continued engagement. The boulder needs to be pushed up the hill by any means necessary. I am, however, urging an interrogation and rethink of civil society's modes of advocacy for meaningful regulatory frameworks, especially since we're operating from a structural disadvantage. Although the AIC's statements were heartening for civil society resisting the OSA, in hindsight they might have also worked to further centralise state power over the digital space and strengthen the channels of communication between the state and Big Tech. The transparency that civil society demands of both tech companies and states should not be compromised for incremental change — especially if such change comes at the cost of inadvertently betraying causes and solidifying the opacity of these public-private engagements.

As Sri Lanka's new National People's Power government embarks on its own trajectory of digitalisation with bold promises of a new "digital economy", SAFEWebLK and the OSA should be homegrown cautionary tales of executive power and corporate-state solidarity for profit. Anti-tech nationalism has been replaced with the more attractive e-nationalism: unique digital IDs, data monopolisation and centralisation, biometrics, and surveillance architecture will soon become part of economic development strategies.

We should learn from developments elsewhere: India's Aadhaar, the world's largest biometric ID system, is a well-covered example of [how "Big ID" has failed people](#) and exacerbated structural discrimination — sometimes to the point of costing people their lives.⁸ Given these problems, it was a cause for serious concern to see Aadhaar's chief technology officer at the [2025 Sri Lanka Digital Public Infrastructure Summit](#), sharing the stage with a plethora of private telecommunications companies, banks and lenders, and the digital economy ministry. Digital rights groups and activists were notably absent at the event. The dialogue had been facilitated by the United Nations Development Programme (UNDP), who also promoted the event aggressively on their websites. The elite capture of such a discussion was clear. The UNDP can hardly be considered a civil society organisation, much less a representative of Sri Lanka's civil society sector. Furthermore, the Ministry of Digital Economy is headed by the country's president, and its senior advisors consist of former private telecommunications bigwigs. Little concern was raised about the potential for executive overreach and the opacity around the development of public-private partnerships shaping Big ID architecture.

At the time of writing, consultations to amend the OSA, once again, have yet to materialise. When they do, they shouldn't be closed-door discussions; they need to be open for public comment and involvement to be meaningful. The continued opacity around the inner workings of the state's digital public infrastructure plans are worrying; economic development cannot once again be grounds for public-private power consolidation to trump people's right to safety and privacy. This should especially be the case for a political party that secured its victory on the back of the people's demands for systemic change. We cannot simply depend on politicians to do the right thing. Civil society will have to, once again, take on the responsibility of pushing for and facilitating transparency. 

WRITER BIO:

Saritha Irugalbandara is a queer feminist from Sri Lanka. Their analysis, writing and activism lies at the intersection of gender, technology, expression and accountability.

END NOTES

1. **Online Safety Act: Media Ministry moves amendment process.** Pamodi Waravita, *The Morning*, 19 January 2025. <https://www.themorning.lk/articles/Srw0xL7s70sJiNx8svdL>
2. **Sri Lanka: Online Safety Act major blow to freedom of expression.** Amnesty International, 24 January 2024. <https://www.amnesty.org/en/latest/news/2024/01/sri-lanka-online-safety-act-major-blow-to-freedom-of-expression/>
3. **Gendered Dimensions: A Critical Look at the Online Safety Act of Sri Lanka.** Shannon Hardy, *Oxford Human Rights Hub*, 6 June 2024. <https://ohrh.law.ox.ac.uk/gendered-dimensions-a-critical-look-at-the-online-safety-act-of-sri-lanka/>
4. **Online Safety Act to be Amended.** Lankasara, 22 January 2025. <https://lankasara.com/news/online-safety-act-to-be-amended/#:~:text=The%20Act%20was%20first%20published,online%20safety%20legislation%20file%20cases.>
5. **White Paper: Digital Governance and Rights in South Asia, and the Path Forward.** Tech Global Institute, February 2025. <https://techglobalinstitute.com/wp-content/uploads/2025/02/Digital-Governance-and-Rights-in-South-Asia-and-the-Path-Forward.pdf>
6. **Tech layoffs ravage the teams that fight online misinformation and hate speech.** Hayden Field and Jonathan Vanian, *CNBC*, 26 May 2025. <https://www.cnbcm.com/2023/05/26/tech-companies-are-laying-off-their-ethics-and-safety-teams-.html>; **Content Moderation in Under-resourced Regions: A case for Arabic and Hebrew.** Tech Global Institute. <https://techglobalinstitute.com/announcements/blog/content-moderation-arabic-hebrew-in-under-resourced-regions/>
7. **Sri Lanka: AIC Media Statement on the gazettal of the Online Safety Bill.** Asia Internet Coalition, 28 September 2023. <https://aicasia.org/download/819/>
8. **India's Aadhaar proves Big ID is still a bad idea.** Access Now, 5 October 2021. <https://www.accessnow.org/press-release/indias-aadhaar-big-id-bad/>





FROM RECRUITMENT TO RESISTANCE

When it comes to fighting radicalisation, fixing the tech is only one piece of the puzzle

An interview with Aizat Shamsuddin, the founder of Initiative to Promote Tolerance and Prevent Violence ([INITIATE.MY](https://www.initiate.my)), on how technology has allowed radicalisation efforts to scale up, and what needs to be done to address the problem.

Balance: Let's start with your background: What drew you into this work on violent extremism and tech?

► I've been working in the prevention of violent extremism space for over a decade now. I started by exploring why people join extremist groups, initially looking at more traditional, offline paths of radicalisation: religious gatherings, lectures at universities, face-to-face indoctrination. But, over time, that focus has shifted towards online radicalisation: social media, messaging apps and other digital tools have now become heavily involved in the recruitment process.



Aizat Shamsuddin, founder of Initiative to Promote Tolerance and Prevent Violence (INITIATE.MY)

My own story is part of that. I was once radicalised myself. I was part of a group that spread hate and division, and I subscribed to those ideas. But I reached a point where I saw through it — how religion and identity were being exploited. That personal experience, paired with my background in law and security, pushed me to help others understand this process and advocate for better responses to it.

With your personal experience, you must see tech's role very differently. Online platforms are often blamed for extremist recruitment. Does solving the tech issue solve the radicalisation issue? How does that intersect with what you've studied around persuasive tech — how does it compare to traditional forms of recruitment?

► Solving the tech issue doesn't solve radicalisation. It goes deeper than that. Radicalisation is a complex process rooted in real-world grievances — identity, injustice, exclusion. Technology doesn't cause it, but it amplifies it. Platforms become tools — enablers that make recruitment faster, broader, and more emotionally charged.

In the past, radicalisation happened in physical spaces — religious classes, kinship circles, peer groups. It was personal. Now, with platforms like Telegram, WhatsApp and social media, extremist networks can scale those same dynamics. Encrypted chat groups mimic real-world intimacy: people talk about their day, what they're cooking, share frustrations. Over time, radical messages are layered into that trust and familiarity. It's subtle but powerful.

At the same time, tech platforms and algorithms quietly reinforce those pathways. You no longer have to seek out extremist content — it finds you. Based on what you engage with, the system feeds you more of the same. That's persuasive tech in action: creating a radicalising environment without coordination, often without people realising they're in one.

So yes, tech speeds things up — it adds scale, emotion and persistence. But unless we address the root causes — alienation, marginalisation, grievance — tech will remain just a powerful tool, not the origin.

You no longer have to seek out extremist content — it finds you.

AI is also accelerating things. Have you seen it affecting how radical content is created or spread?

► Absolutely. Generative Artificial Intelligence (Gen AI) speeds up how messages are crafted and shared. During the Gaza conflict, we saw women using AI-generated images of themselves as warriors — something we hadn't seen before. It's a form of imagined solidarity. While not necessarily radical, it reflects how political identities and affiliations are being reimaged through new tech. Terror groups are also exploiting these tools to enhance their operations and messaging.

Who's pushing these messages? And what makes up this "radicalising environment" you mentioned earlier?

► It's a mix. Sometimes it's coordinated — organised groups deliberately spreading propaganda and hate. But often it's uncoordinated behaviours amplified by algorithms. For example, someone expressing racially or religiously supremacist views gets algorithmically fed more of the same content. That expands the audience well beyond just the already radicalised; it pulls in casual viewers and creates a self-reinforcing loop.

That's what we mean by a "radicalising environment". It's not just about bad actors — it's the structure of the system itself. It can normalise extreme views, isolate people from broader perspectives and push them further down that path.



And what about the far-right? You've done work looking at those influences, too, right?

► Yes. For too long, the world has focused on Islamist extremism — especially after 9/11. But since the Christchurch attack and the rise of neo-Nazism, there has been greater awareness of far-right extremism. What's striking is how these ideologies localise. In Southeast Asia, we've seen versions of racial and religious supremacy adapted to local contexts: East Asian supremacy in Singapore, Malay-Muslim majoritarianism in Malaysia, nationalist narratives in Indonesia. It's evolving and we need to pay attention.

Can you tell me more about INITIATE.MY?

► We formalised INITIATE.MY in 2020–2021, in response to rising inter-group tensions after Malaysia's general election in 2018. We saw a spike in racial and religious hate, but there was little data to back up public concerns. So we began documenting and quantifying cases, turning trends into graphs and analysis. That became our core: a data-driven approach to understanding and countering extremism.

Radicalisation is a complex process rooted in real-world grievances — identity, injustice, exclusion. Technology doesn't cause it, but it amplifies it.

We now work with civil society, law enforcement and regional networks — offering research, training and policy support. Evidence has enabled us to engage more effectively, especially with institutions.

Do you feel hopeful? Are there signs of progress?

► I'm quite pessimistic about this, but we have some solutions. Our flagship programme, Peace Lab, trains participants in content creation and critical thinking. We've even brought in platforms like TikTok to show how positive actors can leverage algorithms, not just be hurt by them.

We've also briefed companies like Meta and TikTok on emerging threats — sharing keywords, contextual cues and trends to inform their policy teams. But the shift to AI-based moderation is worrying. From our experience, current AI systems still struggle with sarcasm, coded language and cultural nuance. They can't replace human moderators — especially not in high-risk areas like extremism.

What keeps you going?

► Honestly, despite the challenges, this is what I care about. I think we all have our own passion about what we want to do in our life. And I guess this is my passion. It sounds cliché, but I think this is something that I'm good at. I've invested more than a decade in this work. And I see others doing the same thing, too — human rights defenders, digital rights advocates, researchers wanting to do good for the world. In a world sliding into greater polarisation and violence, I think it's vital that we all keep pushing back.🇲🇾

BIO:

Aizat Shamsuddin is the founder of Initiative to Promote Tolerance and Prevent Violence (INITIATE.MY).



Platform Power and Populism:

The architecture behind Hindu nationalism's digital rise



IMAGE CREDIT: PRESS INFORMATION BUREAU

Prime Minister Narendra Modi waving at BJP supporters in Daman, a union territory in western India.

by **AISHIK SAHA**

In India, the rise of Hindu nationalism isn't just a political story—it's a digital one. Aishik Saha unpacks how the BJP has mastered the mechanics of the internet's attention economy, using social media, algorithmic amplification and ad-tech monopolies to manufacture consent, suppress dissent and dominate discourse. Disinformation isn't a glitch in the system—it is the system, fueled by market incentives and platform logic. Tracing a line from grassroots mobilization to click farms and vigilante publics, this piece reveals how digital capitalism and political ideology have merged, and why reimagining the infrastructure of the internet is now a democratic imperative.

The electoral dominance of Hindu nationalism in India is often explained through the Bharatiya Janata Party's (BJP) success in socially engineering mass support via its vast and deeply embedded organisational apparatus. But while this explanation rightly foregrounds the historical role of grassroots mobilisation and ideological dissemination, it fails to sufficiently account for the dramatic transformation of India's political communications landscape in the digital age. Narendra Modi's rise from political relegation after the 2002 anti-Muslim riots in Gujarat state to the leading prime ministerial candidate in 2014 — and eventual victory — has been at least partly [ascribed to the use of social media for election campaigning](#). (Frances Haugen, the former Facebook employee and whistleblower, has also [talked about the platform's behaviour in India](#), particularly in relation to the pressure they feel from the Indian government.¹)

It's become increasingly clear that part of the support for Hindu nationalism in online spaces is inauthentic, but the way this inauthenticity allows political momentum to coalesce around it reveals plenty about how sociotechnical systems are embedded into the internet.

As the World Wide Web gained popularity, user attention increasingly became a proxy for capital. The concept of the "attention economy", first formulated in the 1990s, has become a critical lens through which the commodification of human attention in the digital age can be understood.² It treats attention as a scarce, measurable resource — something to be captured, traded and exploited. And in today's landscape, dominated by monopolistic tech platforms and algorithmic content curation, the competition for attention is no longer about providing superior goods or services but rather about gaming visibility. This has resulted in a grey market of digital manipulation: fake reviews on e-commerce platforms, purchased 'likes' and followers on social media, bot amplification of content and more.

Hindu nationalism's online ascendancy did not emerge out of a vacuum; it has come about in an environment where inauthenticity can simulate public will and where disinformation functions as an organic product of market incentives.

Clickbait, for example, is a well-known tactic in the struggle for attention. It thrives particularly in moments of institutional breakdown, such as the current crisis of trust in the mainstream media. Sensational headlines and viral hoaxes erode journalistic standards, foster distrust and reduce news to the presentation of never-ending spectacles. This creates fertile ground for a digital economy of networked disinformation (or DEND) — an ecosystem where low-cost, low-rigour content, often produced by precarious digital labour, intersects with platform logics of engagement and virality. Many DEND websites derive their income from ad revenue, incentivising the use of polarising content to funnel traffic from sympathetic social media pages. A post from one page can cascade through dozens of others, crafting a distributed yet coordinated disinformation apparatus. In this way, networks can mount large-scale disinformation campaigns with maintaining financial viability through economics of scale.

It's of no surprise that India's ruling BJP has emerged as a champion and political beneficiary of the discourse on digitisation and digital governance, especially as internet penetration has increased in India over the last decade. The party has managed to not only effectively dominate online political discourse but also reshape the discourse itself. These days, even opposition parties, eager to move with the political winds, [toe the line on 'soft' Hindu nationalism](#).

This has been partly achieved through disinformation campaigns created by paid producers willing to spread disinformation in exchange for money or other forms of access to power. Facts have taken a beating in the attention economy; it's content that can generate the most outrage that dominates now. Whether that content is accurate, balanced or fair is no longer a consideration for those who prioritise virality and influence. Combine this with Hindu nationalism and one gets a heady mix primed for political weaponisation.

In her paper, *Vigilante Publics: Orientalism, Modernity and Hindutva Facism in India*, Shakuntala Banaji, a professor of media, culture and social change at the London School of Economics, noted that, since the 1990s, the rise of Hindu nationalism has been accompanied by a visual performance combining narratives of economic growth with a cultural revival of a mythical Hindu past.³

Social media has given this a further boost, allowing users to participate in the ‘spectacle’ while maintaining a semblance of autonomy, thus creating an illusion of popular support and participation. A [report by the Center for the Study of Organized Hate](#) on ‘cow vigilantism’ — mob-based violence perpetrated by Hindus against non-Hindus (usually Muslims) in the name of protecting cows, a sacred animal in Hinduism — shows how online hate can be translated into spectacles of routinised physical violence.⁴ Acts of vigilante violence are often uploaded on social media as a form of legitimisation and even ‘accountability’ to people who can, in turn, support such activity through online engagement and financial support. An online presence, therefore, has become increasingly integral to performances of vigilantism. Between the BJP and social media algorithms, state patronage and online visibility have been transformed into tools for manufacturing popular support for literal highway robbery and violence.

The failure of tech companies to uphold their own content policies and standards has also played into the hands of populist parties like the BJP. Hindu nationalist websites [monetise their content](#) through Google Ads as well as advertising platforms like Taboola, Microsoft’s AppNexus and iZooto. While much of the content on these websites clearly violate the platforms’ policies, the nature of programmatic advertisements — combined with [Google’s monopoly over the adtech stack](#) — means that, when Google fails to enforce its own terms, advertisers have practically no means to stop funding online hate. The only thing they can do is withdraw from Google Ads completely, but our digital age makes that not a viable option for many businesses.

Between the BJP and social media algorithms, state patronage and online visibility have been transformed into tools for manufacturing popular support for highway robbery and violence.

It doesn’t help that this is all happening at a time when mainstream media outlets are going through their own struggles and transformations — and not necessarily for the better. As newsrooms slash budgets or demand more from their employees, journalists have grown more and more reliant on public relations professionals for content and informational support. This means that anyone with the resources to hire PR consultants has more of a chance than ever to shape the news agenda.

Meanwhile, Google’s PageRank algorithm has done more than just organise the internet; it’s also [transformed the web into a marketplace of attention](#). By assigning a measurable value to each link in a vast digital network, PageRank effectively converts social and informational relationships into traceable metrics. Algorithmic biases mean that the diversity of content available to a user is incrementally lowered, forming filter bubbles. In the struggle to maintain reader traffic and relevance, media organisations are increasingly incentivised to chase the sorts of headlines and news items that ‘please’ the algorithm and get them ranked higher than their competitors. Hindu nationalist organisations like BJP have been able to leverage these structures to exert increasing control over the information environment.

That isn’t all. Apart from shaping media agendas, the BJP is also slowly and steadily coming to dominate mainstream and legacy media networks themselves. The emergence of the twenty-four-hour news cycle in the 1990s created a hyper-competitive news market in India; instead of focusing on issues impacting the broadest section of the Indian population, media houses competed for ratings by pandering to the most affluent sections of the urban upper and middle class. They did this through [a process of “Bollywoodisation”](#), defined as “celebratory media dominated by breathless gossip about cricketers, billionaires and Bollywood stars and point-scoring among the political elite”.⁵



Even before social media entered the game, the Indian mainstream media was already growing more and more preoccupied with gossip, scandal and spectacle — making them all the more vulnerable to the tactics of populists in an attention economy.

At first, the BJP embarked on a long-term project to delegitimise independent journalism, labelling any criticism of Modi as coming from “anti-national”, elitist media, part of a “liberal cabal”. But, after their 2014 election victory, the BJP began to dominate the mainstream and alternative media agenda. Reliance Industries, owned by the BJP-aligned oligarch Mukesh Ambani, acquired control over major media conglomerates such as Network18, thereby consolidating pro-government influence on both television and digital platforms. The rise of compliant media houses like Republic TV, Zee News and Aaj Tak — all of whom have uncritically repeated Hindu nationalist talking points — further cemented the hegemonic process. In their rush for attention and willingness to collaborate with Hindu nationalists, these media houses have run false stories — claiming that “rate cards” had been issued offering payment for converting women to Islam, or spreading hoax reports of attacks on Hindu temples — seemingly without scrutiny or independent investigation. Such media reports further serve to legitimise disinformation users may have received from other sources, and the vicious cycle continues.

The BJP’s political dominance cannot be separated from the structural logics of digital capitalism, particularly the monopolistic architectures of attention, advertising and algorithmic mediation. Hindu nationalism’s online ascendancy has not emerged in a vacuum; it has come about in an environment where inauthenticity can simulate public will, and where disinformation functions not as a disruption but as an organic product of market incentives.

The BJP’s political dominance cannot be separated from the structural logics of digital capitalism, particularly the monopolistic architectures of attention, advertising and algorithmic mediation.

The collapse of editorial standards, the rise of vigilante publics and the emergence of a digitally enabled ideological economy illustrate a broader systemic crisis. Under such conditions, algorithmic visibility and capital flow determine the overall expression of public opinion.

Yet, precisely because this environment is a constructed one, it can also be reimagined. If we accept that the current system amplifies hate, suppresses dissent and reduces democratic participation to a monetised spectacle, then the need to imagine alternatives is not utopian but necessary. This begins by addressing the infrastructural monopolies that allow political and economic elites to define the limits of public discourse. It also calls for a reconstitution of the digital public sphere from opaque ad-driven platforms to accountable, decentralised infrastructures that prioritise informational integrity over engagement metrics.⁵

WRITER BIO:

Aishik Saha is a Trust and Safety Researcher at the Centre for the Study of Organized Hate. He specialises in networked disinformation, digital policy, particularly around the Digital Services Act, Online Safety Act, and online content regulation.

END NOTES

1. How Advertisers and Investors Can Push Social Media Platforms to Curb Hate Speech and Disinformation. Deeksha Udupa, Center for the Study of Organized Hate, 2 November 2024. <https://www.csohate.org/2024/11/02/frances-haugen-big-tech-accountability/>
2. The attention economy and the Net. Michael H. Goldhaber, First Monday, 7 April 1997. <https://firstmonday.org/ojs/index.php/fm/article/view/519>
3. Vigilante Publics: Orientalism, Modernity and Hindutva Facism in India. Shakuntala Banaji, *Javnost - The Public*, 2018. <https://www.tandfonline.com/doi/full/10.1080/13183222.2018.1463349>
4. Streaming Violence: How Instagram Fuels Cow Vigilantism in India. Center for the Study of Organized Hate, 19 November 2024. <https://www.csohate.org/2024/11/19/instagram-fuels-cow-vigilantism-in-india-report/>
5. An Uncertain Glory: India and its Contradictions. Jean Drèze and Amartya Sen, Princeton University Press, 2013.



DOCUMENTING RESISTANCE, BUILDING ALTERNATIVES

The App Censorship Project and the struggle for digital freedom in Asia

by **BENJAMIN ISMAIL**

From app removals in China to quiet compliance in Hong Kong, Benjamin Ismail traces the rise of platform-enabled censorship and the complicity of global tech giants in enabling digital authoritarianism. He unpacks the findings and ambitions of the App Censorship Project, an initiative working to expose the opaque practices of Apple and Google, and to push for transparency, accountability and a more just digital future.

Across Asia, digital authoritarianism has increasingly tightened its grip on online freedoms, restricting access to information and communication through a combination of heightened surveillance, mandates on internet infrastructure providers and strategic cooperation with global technology platforms. Governments across the region are leveraging the centralised control of mobile ecosystems to enforce censorship with unprecedented precision and scale.

Mobile devices are now the primary gateway to the internet for billions of people, which means that platforms like Apple's App Store and Google's Play Store have become critical arbiters of online speech and access. Once seen as gateways to innovation, these app distribution monopolies are now also tools of suppression used by authoritarian regimes to remove apps that offer privacy, secure communication or access to independent media. By complying with takedown requests, tech giants become complicit in enabling censorship, eroding fundamental rights and silencing dissent.

A PLATFORM FOR TRANSPARENCY AND ACCOUNTABILITY

■ The App Censorship Project officially launched in 2023, but its origins trace back to the creation of AppleCensorship.com in February 2019. Since its inception in 2008, Apple's App Store had operated as a black box with little public understanding of how or why apps were removed. AppleCensorship.com was thus born out of the need to expose the opaque nature of the company's app curation process and force transparency into an ecosystem that had long evaded scrutiny.

The catalyst for the initiative was Apple's intensifying cooperation with the Chinese government. Censorship escalated following Apple's entry into China in 2010. One of the first major app removals involved politically sensitive figures like the Dalai Lama and Uyghur leader Rebiya Kadeer. In 2013, Apple removed FreeWeibo, an app we created to archive censored Weibo posts, further illustrating the company's growing complicity.

By 2017, Apple's compliance reached a new height: over 600 Virtual Private Network (VPN) apps were removed from its China App Store after demands from Chinese authorities. This mass takedown was the first categorical ban of its kind in a major app store, executed with little public disclosure. Following minimal pushback from legislators and the media, Apple resumed business as usual.

This set the stage for AppleCensorship.com, a real-time monitoring platform powered by the App Store Monitor (ASM). The ASM tracks app availability across all 175 of Apple's App Stores, providing a searchable and systematic record of removals.

While Apple was the initial focus, Google's Play Store also plays a critical role in the app distribution ecosystem. Recognising the need for comprehensive monitoring, the App Censorship Project expand-



THE EPICENTRE OF PLATFORM-ENFORCED CENSORSHIP

■ China stands at the centre of this new model of censorship. As mentioned, it wasn't long after Apple entered the Chinese market that they began engaging in political filtering. When U.S. senators criticised their sweeping 2017 ban of VPNs from the Chinese App Store, the company insisted that it was merely complying with local laws. It was the first known instance of a platform executing a full “categorical ban”. VPNs, essential for circumvention and privacy, were entirely blocked in China.

In the years since, Apple has continued to quietly remove apps deemed objectionable by Chinese authorities. As of June 2025, the ASM has logged 18,801 unavailable apps in the China App Store — an astonishing 28.12% unavailability rate, more than double the global average. The apps more affected include those relating to news, books and social networking. Apps touching on religion, LGBTQ+ issues, Tibet or Uyghur identity are consistently targeted. The result is a tightly controlled digital environment where even basic information tools are inaccessible.

A 2023 analysis comparing the 100 most downloaded apps worldwide found that sixty-six were unavailable to iOS users in China. Just four of the top 100 global apps appeared on China's “most downloaded” list — all four were domestic Chinese services. By contrast, only eight of the top 100 apps were unavailable in the U.S. App Store. This illustrates the unprecedented level of digital isolation faced by Chinese users.

Despite facing increasing repression since the 2014 Umbrella Movement and an intensified crackdown beginning in 2019, Hong Kong has not yet mirrored the extreme app censorship of mainland China. Still, the situation is far from reassuring — it's still significantly more re-

ed in 2024 with the launch of GoogleCensorship.org, powered by the Play Store Monitor (PSM). This expansion allows comparative analysis across both dominant mobile platforms, exposing censorship trends and regional disparities.

The forthcoming AppCensorship.org will serve as an aggregated hub, bringing together datasets from both AppleCensorship.com and GoogleCensorship.org to deliver a holistic view of app suppression worldwide. The idea is to enable cross-platform transparency, support advocacy efforts and inform digital rights strategies.

TURNING DATA INTO ACTION

■ Despite the immense size of Apple and Google's app stores — each hosting around two million apps — what initially seemed like a needle-in-a-haystack search for censorship quickly revealed deeper patterns. Repeated digging uncovered systematic and politically driven restrictions. We observed a clear and consistent unavailability of LGBTQ+ apps across much of the Middle East and Gulf region, and came to understand just how profoundly isolated China's App Store is from the rest of the global ecosystem. Our research also brought to light a range of situations, including in Russia and Hong Kong, where Apple compromised its publicly stated commitment to human rights in response to state demands or regional pressures.

One particularly striking example occurred last summer, when Apple quietly removed more than 60 VPN apps from the Russian App Store under orders from Roskommnadzor, the Russian federal agency overseeing mass media in the country. These ‘silent’ takedowns severely limited Russian users' ability to access secure web services and communicate freely.

strictive than stores in countries we classify as “free”.

In late 2022, we began assessing the Hong Kong App Store, using data from both AppleCensorship.com and external sources. Our report, *Apps at Risk: Apple’s censorship and compromises in Hong Kong*, examined Apple’s compliance with censorship demands in the Special Administrative Region. Many residents rely on apps that are banned in mainland China to access information and communicate — as the master of the App Store, Apple could potentially become a ‘kill switch’ for censors.

We found that Apple, likely under pressure from Hong Kong authorities or the Chinese central government, had already repeatedly removed apps deemed illegal or politically sensitive. As of November 2022, more than fifty VPN and private browsing apps have already disappeared from the Hong Kong App Store. The report also noted the global removal of several news and media apps, suggesting that Apple may be engaging in pre-emptive self-censorship or acting on behalf of authorities. Crucially, Apple has never made a public commitment to safeguarding Hong Kong residents’ digital rights, leaving its future stance on censorship under pressure highly uncertain.

NO SIMPLE CORRELATION

■ A key observation from our research is that there’s no direct correlation between a country’s broader digital authoritarianism and the state of its app distribution platforms, whether it’s Apple’s App Store or Google’s Play Store. For example, Vietnam has heavily cracked down on independent journalism, civil society forums and political bloggers, yet we have found no significant app takedowns. The same applies to Laos, Cambodia and, to a lesser extent, Pakistan.

There are several plausible — but difficult to verify — explanations for this.

First, a low perceived threat: authorities in these countries may view app-based platforms as less significant due to low user engagement or mobile penetration and therefore see no need to interfere.

Second, failed or filtered takedown attempts: as suggested by Apple’s 2018 transparency reports, governments may have submitted removal requests that lacked proper legal justification or focused solely on non-political content (for example, illegal gambling, child exploitation or drug-related apps).

Finally, corporate resistance: in some cases, tech companies may exert enough economic and political leverage to dissuade local authorities from issuing such requests.

Given the opacity surrounding both state action and corporate compliance, these patterns are difficult to confirm definitively, but the data nonetheless highlights important trends.

Some countries do show growing signs of platform-based censorship, particularly on the Google Play Store. In Myanmar, the military junta has increasingly tried to control the flow of information online. In India, under Prime Minister Narendra Modi’s administration, there have been documented attempts to suppress dissent and restrict content online.

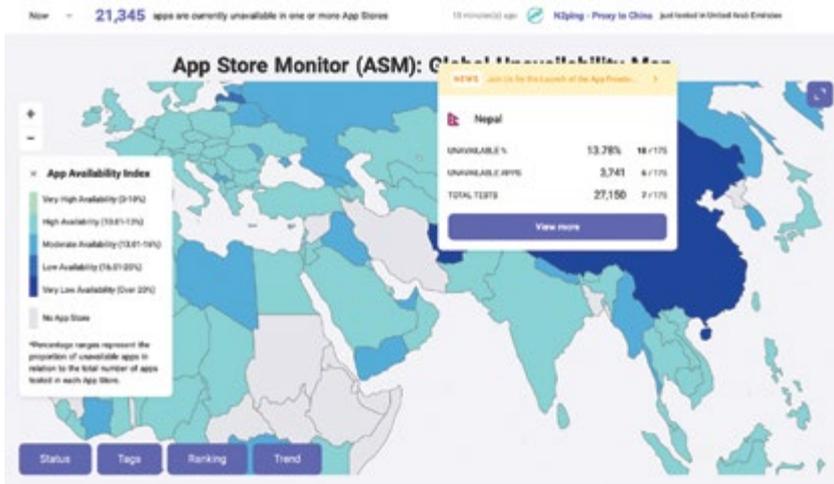
Both countries exhibit a higher rate of app unavailability on Android platforms, which is significant given that the majority of users in these countries use Android over iOS. This suggests that censorship strategies are increasingly adapting to local user demographics and platform dominance.

BUILDING A JUST AND RESILIENT DIGITAL FUTURE

■ The App Censorship Project isn’t confined to observation and documentation; it’s fundamentally an initiative for systemic transformation. Drawing from its research and on-the-ground findings, the Project advances a series of bold and actionable reforms aimed at reshaping the digital ecosystem into one that’s more transparent, accountable and just.

One of the Project’s central demands is for mandatory transparency reporting: technology giants such as Apple and Google should be required to publish detailed disclosures of all app removals, including the specific reasons for each takedown and the jurisdictional contexts in which they occur. Such transparency is essential for meaningful public oversight and accountability.

App stores have become silent enforcers of censorship — their opaque decisions shape what billions can access, with little accountability and profound consequences for digital freedom.



Screen grab from <https://appcensorship.com> showing the App Store Monitor censorship levels across the world.

Beyond disclosure, the Project advocates for the establishment of independent oversight mechanisms. These would take the form of third-party bodies with the authority to review, challenge and potentially overturn app removal decisions, thus ensuring that such actions align with international human rights standards rather than opaque corporate or governmental interests.

The Project also calls for legal protections for sideloading and the development of alternative app stores everywhere. We need to dismantle the monopolistic control of dominant platforms. By enabling users and developers to access and distribute apps through open, competitive channels, these reforms would reinforce digital autonomy and innovation.

Finally, the Project urges investment in decentralised and community-governed platforms. Federated, open-source technologies, built and maintained by communities rather than corporations, offer resilient alternatives to centralised gatekeepers. These tools not only resist censorship and surveillance but also foster inclusivity and democratic governance in the digital sphere.

Together, these proposals form a blueprint for a more equitable digital future, one in which corporate complicity is challenged, user agency is restored and civil society is empowered to shape the digital spaces it inhabits.

TOWARDS DIGITAL FREEDOM IN ASIA... AND BEYOND

■ The App Censorship Project represents more than resistance — it embodies a proactive vision of digital autonomy and resilience. By combining rigorous documentation, targeted advocacy and visionary proposals, the Project provides a comprehensive framework to not only challenge but dismantle centralised digital gatekeeping.

As governments escalate digital control, transparency and accountability will be essential to safeguarding online freedom.

Ultimately, the success of this effort hinges on global cooperation, meaningful policy reform and sustained grassroots resistance. While

regulatory change may be difficult to achieve in many local contexts, there remains significant potential for impact in jurisdictions such as the United States — where major tech companies are headquartered — and in the European Union, where there’s been a growing willingness to confront platform power through legislation.

To that end, it’s essential that civil society actors and digital rights defenders in countries facing rising digital authoritarianism recognise the urgent threat posed by Big Tech’s unchecked gatekeeping power. These corporations operate with virtually no transparency obligations and little to no accountability mechanisms, yet their decisions shape access to information on a global scale. The risks they pose are not confined to any single region; they imperil the future of the open internet everywhere and contribute to the accelerating fragmentation of the internet into national or corporate-controlled silos, undermining its universality and openness.

Through its relentless monitoring and bold reform agenda, the App Censorship Project is working to ensure that digital freedom remains not just an ideal but a concrete possibility, both for Asia and for the world at large. 🇧🇪

WRITER BIO:

Benjamin Ismail is Campaign and Advocacy Director at GreatFire and leads the App Censorship Project. A long-time advocate for freedom of information, he previously worked with Safeguard Defenders and led Reporters Without Borders’s (RSF) Asia-Pacific desk, where he spent seven years campaigning against censorship in China and other authoritarian regimes.



Send
messages, not
metadata

SESSION

No phone numbers. No emails.
Just encrypted messages.



CONTRIBUTE TO
BALANCE





Campaigns, Clicks, and Complicity

How civil society actors built the 'buzzer' industry

by PRADIPA P. RASIDI

In this essay, Pradipa P. Rasidi traces how Indonesia's pro-democracy volunteers and civil society actors helped build the country's digital influence industry. Drawing on years of research and firsthand experience, Rasidi explores how platform power, class interests and political ambition converged to shape a distinctly local form of digital colonialism.

It was March 2015 when Yani (not his real name), a senior figure in Indonesia's pro-democracy movement, insisted that then-President Joko Widodo had become too important to be challenged. The meeting I attended, initially focused on local bureaucratic reformers, shifted to defending Jokowi, as Widodo is popularly known. Despite growing controversy, he was celebrated as a reformer from the provinces who rose to become president. At that time, less than a year into his presidency, Jokowi had nominated his party's confidant as the national police chief even though that individual was suspected of bribery; this was seen as his [first move against anti-corruption efforts](#).¹ Yani, though uneasy, urged continued support of Jokowi and close oversight of his volunteer networks.



Indonesia has seen its digital influence industry grow dramatically over the past decade.

The volunteers Yani was referring to were a network of middle-class professionals who'd emerged as Jokowi's base since his 2012 Jakarta gubernatorial bid. Rather than fostering civic engagement like in established democracies, they functioned as part of the electoral machinery. Drawn by Jokowi's image of humility and distance from political-economic elites — “a new hope”, as *Time* [dubbed](#) him — they saw in him a figure capable of pushing back against the entrenched oligarchy.² Jokowi's volunteer-driven campaign was largely mobilised online and included endorsements from prominent civil society actors — activists, NGO workers and journalists — such as Goenawan Mohamad, the founder of the magazine *Tempo*, and Teten Masduki, a social activist who later [became](#) the Presidential Chief of Staff.³ These volunteers were widely credited with helping secure Jokowi's 2014 victory.⁴

The digital mobilisation they pioneered did more than elect a president. From analytics and algorithmic optimisation to sockpuppet account deployment, their methods seeded what would become Indonesia's sprawling influence industry: an oligarch-financed, extra-state apparatus dedicated to shaping perception and silencing dissent. These tactics would later help propel Jokowi's rival-turned-protégé, Prabowo Subianto, to the presidency in 2024. There was a time, however, when influence operations were seen as fair play among activists. Based on my experience working in Transparency International Indonesia from 2014 to 2017, as well as ethnographic interviews and fieldwork with influence operators carried out at various points between 2016 and 2023, this piece situates that moment through the rubrics of digital colonialism.⁵

The crux of digital colonialism is not just about domination from afar; it's also about the tenuous capture of power.

DIGITAL COLONIALISM AND ITS LOCAL INTERMEDIARIES

● The notion of digital colonialism has emerged as a critique from scholars and digital rights activists, responding to the expansion of tech power from the Global North. Much like historical colonialism, in digital colonialism a handful of powerful actors extract data, labour and value from the Global South and marginalised identities. Whether framed in terms of infrastructure dependency, surveillance capitalism or algorithmic control, [the critique](#) remains: digital technologies reproduce colonial patterns of exploitation.⁶

But much of this critique flattens reality, erasing questions of class and cultural affinities by imagining the South as mere victim, never collaborator. In historical colonialism, empires were always mediated by native collaborators and allies. Far from the national myths of control and resistance, colonial empires often exploited and were exploited by local rivalries. In maritime Southeast Asia, colonial powers [relied](#) on indigenous elites — rulers, aristocrats, merchants and rival factions — to mediate their expansion.⁷ From the sixteenth to eighteenth centuries, Moluccan rulers [allied](#) variously with the Portuguese, Spanish and Dutch, trading spices and slaves in exchange for leverage over local competitors.⁸ Rather than total domination, empires operate through tensions.

This interplay persists in digital colonialism. Platforms like Meta (Facebook and Instagram), Google and Twitter/X capture user behavior and social relations data and feed them into algorithms that optimise content generation and ad targeting. That data is also leased to advertisers and content promoters to improve targeting, monetising attention through detailed profiling. Surrounding this core infrastructure is an ecosystem of social media intelligence and advertising analytics firms. In the United States, firms like Acxiom convert such behavioural data into [“premium proprietary behavioral insights”](#) — clustering users by class, spending and geography — that they sell to government agencies, insurers and other clients.⁹

In Indonesia, these processes are localised by the homegrown influence industry. Political consultants, digital strategists and marketers use platform infrastructures to serve domestic interests. They track online behaviour — trends, sentiment, engagement patterns — and sell these insights to politicians, companies or state agencies. Based on client needs, they then run [“buzzing campaigns”](#) using influencers, sockpuppet accounts, targeted ads and media partnerships to shape public opinion.¹⁰ These campaigns generate organic engagement from users and feed more data back into the platforms' extractive engines. Just as native collaborators once contributed to imperial economic flows, the work of Indonesia's influence industry helps to perpetuate the power of Big Tech platforms.



Digital technologies reproduce colonial patterns of exploitation, whether it be through infrastructure dependency, surveillance capitalism or algorithmic control.

CIVIL SOCIETY'S ROLE IN THE ENGAGEMENT-INDUSTRIAL COMPLEX

● Many civil society actors played key roles in the influence industry's earliest days. Journalists, activists and NGO workers joined Jokowi's 2014 campaign as volunteers, seeing him as a liberal-pluralist reformer, especially against his then-rival, Prabowo, a former general and son-in-law of Indonesia's late dictator.¹¹ Jokowi's victory fed the optimism of a new age of ["digital democracy"](#): a space where ideas could be contested and mobilisation decentralised.¹² But as the mainstream media and his supporters lionised Jokowi, his image eclipsed democratic deliberation — like Yani said, he was perceived to be too important to challenge. What began as a ["nexus of electoral and movement politics"](#) morphed into (manipulative) public relations.¹³

For some, this shift was strategic.¹⁴ Jokowi, it was argued, needed support from below to counterbalance the oligarchs around him. Not only was his campaign driven by social media, his commitment to the idea of "digital transformation" — expanding internet access, digitising state services, funding e-commerce — won further support. For digital rights activists, infrastructure access had [long been a concern](#).¹⁵ Rural areas were often framed as "underdeveloped", and internet access was treated as an unquestioned good after neglect under previous administrations. Furthermore, many civil society organisations tended to [rely on lobbying](#) and championing political reformers rather than organising for change on the ground.¹⁶ Jokowi's outsider status and pluralist commitment played into an "orang baik (good person)" narrative that was (mistakenly) equated with liberal politics, [solidifying](#) his appeal to civil society.¹⁷

This fusion of moral idealism and strategic realism drew activists, journalists and NGO workers into influence operations. Some ran sockpuppet accounts or crafted campaign content; others became strategists or influencers.¹⁸ Those at the forefront rebranded themselves as "citizen journalists" or "social media activists". The journalist Pepih Nugraha, for example, built an online brand around narrative investigation, while others peddled insider secrets; such content amassed millions of views.¹⁹ As they cultivated audiences, many also deepened ties with political patrons. When Jokowi crushed the Islamist opposition in 2018 and weakened the anti-corruption commission in 2019, these actors helped shape the narrative, claiming that repressive measures were necessary to prevent Islamic extremism.²⁰ As intermediaries in digital colonialism, they negotiated contracts for their knowledge of platforms, data amplification and political psychographics. They became cultural translators of algorithmic power.

By Jokowi's second term in 2019, these loose networks had transformed into an industry. What began as volunteering for politicians and government agencies had extended to working for conglomerates, state-owned firms and even celebrities.²¹ Jokowi's alliance with Prabowo in his second term blurred old rivalries and Covid-19 accelerated [demand for digital campaigns](#).²² What was once framed as moral engagement had evolved into routinised labour.

Many actors now operate on transactional terms, seeking the highest bidder while maintaining proximity to political-economic elites. This reflects a broader trend of government supporters receiving access, contracts or posts in government agencies or state-owned enterprises — a life path more economically secure than precarious labour in civil society.

WHAT COMES AFTER 2024?

● Today, the links between platform power and Indonesia's political-economic elites are unmistakable. In digital colonialism, the colonised are not passive victims but strategic actors. President Prabowo, who inherited much of Jokowi's digital machinery, hired Noudhy Valdryno, former Head of Public Policy for Meta in Indonesia and Brunei Darussalam, to be part of his 2024 electoral campaign team. After winning the election, Noudhy became Deputy Chief of the Presidential Communications Office, bringing with him operational knowledge and firsthand experience of how the platforms work.²³ The influence industry [continues to expand](#), drawing in a new generation of strategists and operators — some from lower-middle-class backgrounds — hungry for a career path.²⁴

Many in broader civil society, too, are entangled in platforms. There's growing interest in aligning with social media logics — adopting "best practices" in digital activism, treating virality as metrics of success, and leveraging social media as part of



institutional KPIs.²⁵ With Prabowo's strong hold over influencers, rights organisations also increasingly seek collaborations with other content creators to compete for algorithmic attention.

It's a fragile relationship. Influencers may co-opt activism idioms to build legitimacy, then pivot to positions that better serve personal visibility — supporting freedom of expression one day, endorsing anti-labour policies the next. Reliance on platforms also leads to activists becoming enmeshed in the extractive infrastructures they oppose. Platforms reward emotional pull and algorithmic fine-tuning, pulling activist organising towards the logic of individualised attention. Under these rubrics, activism must be optimised — legible, marketable, ready for circulation, analytics and strategic repackaging.

This is the crux of digital colonialism. It's not just about domination from afar; it's also about the tenuous capture of power: from the internalisation of platform logics to the ways in which the colonised seek to act, mediate and communicate. 

WRITER BIO:

Pradipa P. Rasidi is a digital anthropologist and software developer with eight years of experience in Indonesia's civic space. He previously worked at EngageMedia, focusing on digital security, influence operations, and gamification. His research on sociotechnical imaginaries and relations has been published in *HAU: Journal of Ethnographic Theory, Communication, Culture & Critique, ISEAS Perspectives, and Tactical Tech*.

END NOTES

- Indonesia's Political Elites Drive Anti-Graft Agency into Jeopardy. Natalia Soebagio, *The Conversation*, 12 February 2015. <https://theconversation.com/indonesias-political-elites-drive-anti-graft-agency-into-jeopardy-37364>
- The New Face of Indonesian Democracy. Hannah Beech, *TIME*, 15 October 2014. <https://time.com/3511035/joko-widodo-indonesian-democracy/>
- Jokowi & Para Relawan. *Majalah Tempo*, 3 August 2014.
- Compare these articles for two different analyses on volunteers: Civil-Society Support: A Decisive Factor in the Indonesian Presidential Elections in 2014. Ririn Sefrani and Patrick Ziegenhain, *ASIEN: The German Journal on Contemporary Asia*, July 2015. <https://doi.org/10.11588/asien.2015.136.18949>; The Myth of Civil Society's Democratic Role: Volunteerism and Indonesian Democracy. Hurriyah, *Jurnal Politik: Jurnal Ilmu Politik*, 2019. <https://doi.org/10.7454/jp.v4i2.1045>
- Thank you in particular to my friends and colleagues, Shinte Galeshka and Ahmad Sajali, whose insights during my time in civil society shaped a significant part of the ideas presented in this article.
- The Costs of Connection: How Data Is Colonizing Human Life and Appropriating It for Capitalism. Nick Couldry and Ulises A. Mejías, Stanford University Press, 2019. <https://doi.org/10.15036/0360-3660%E2%80%910>; Digital Colonialism: The Evolution of US Empire. Michael Kwet, Longreads, 4 March 2021. <https://longreads.tni.org/digital-colonialism-the-evolution-of-us-empire>; Tech Colonialism Today. Sareeta Amrute, EPIC2019 Keynote Address, 24 October 2019. <https://points.datasociety.net/tech-colonialism-today-9633a9cb00ad>
- The Dutch and English East India Companies: Diplomacy, Trade and Violence in Early Modern Asia. Edited by Adam Clulow and Tristan Mostert, Amsterdam University Press, 2018. <https://www.jstor.org/stable/j.ctv9hvfq2>
- On the Edge of the Banda Zone: Past and Present in the Social Organization of a Moluccan Trading Network. Roy R. Ellen, University of Hawai'i Press, 2003. <https://www.jstor.org/stable/j.ctvmmxq8>
- Surveillance Capitalism: Monopoly-Finance Capital, the Military-Industrial Complex, and the Digital Age. John Bellamy Foster and Robert W. McChesney, *Monthly Review*, 1 July 2014. <https://monthlyreview.org/2014/07/01/surveillance-capitalism/>

10. Of Play and Good Men: The Moral Economy of Political Buzzing in Indonesia. Pradipa P. Rasidi, in *Digital Technologies and Democracy in Southeast Asia*, edited by Yatus Sastramidjaja, Sue-Ann Lee and Yew-Foong Hui, ISEAS-Yusof Ishak Institute, forthcoming. https://www.academia.edu/49585894/Of_Play_and_Good_Men_The_Moral_Economy_of_Political_Buzzing_in_Indonesia_forthcoming_; Inside the World of Indonesia's Social Media 'Buzzers' Cashing in on Election Propaganda. Anika Burgess and Hellena Souisa, *ABC News*, 20 January 2024. <https://www.abc.net.au/news/2024-01-20/political-buzzers-indonesia-election-misinformation-social-media/103298530>

11. *Majalah Tempo*, 3 August 2014.

12. Temu Demokrasi Digital 2014: Menghimpun Daya, Menentukan Perubahan. *Demokrasi Digital*, archived 16 March 2016. <https://web.archive.org/web/20160316083616/http://demokrasidigital.net/temu-demokrasi-digital-2014/>

13. New Forms of Political Activism in Indonesia: Redefining the Nexus between Electoral and Movement Politics. Dirk Tomsa and Charlotte Setjadjadi, *Asian Survey*, 2018. https://ink.library.smu.edu.sg/soas_research/2719/

14. The continued support for Jokowi from civil society was not without contention, attracting criticism from human rights and anti-corruption organisations, two fields seen as having been sidelined since Jokowi's first years in power.

15. NGOs, the Internet and Sustainable Rural Development: The Case of Indonesia. Yanuar Nugroho, *Information, Communication & Society*, 2010. <https://doi.org/10.1080/13691180902992939>

16. Indonesia Demonstrates That Civil Society as a Backbone of Democracy Is a Myth. Abdul Mughis Mudhoffir, *Melbourne Asia Review*, 8 November 2022. <https://www.melbourneasiareview.edu.au/indonesia-demonstrates-that-civil-society-as-a-backbone-of-democracy-is-a-myth>

17. Symposium Jokowi: Pebisnis Politik Menggapai Indonesia Emas. Riwanto Tirtosudarmo et al, *Tonggak Pustaka*, 2025; Southeast Asia's Troubling Elections: Nondemocratic Pluralism in Indonesia. Edward Aspinall and Marcus Mietzner, *Journal of Democracy*, October 2019. <https://doi.org/10.1353/jod.2019.0055>

18. Some journalists joined buzzing campaigns independently of their media affiliations while some others are affiliated with media organisations directly involved in orchestrating such campaigns. Compare: Ludic Cybermilitias: Shadow Play and Computational Propaganda in the Indonesian Predatory State. Pradipa P. Rasidi, *Communication, Culture & Critique*, December 2023. <https://doi.org/10.1093/ccc/tcad020>; Memetic Persuasion and WhatsApp Application in Indonesia's 2019 Presidential Election. Emma Baulch, Ariadna Matamoros-Fernández and Fiona Suwana, *New Media & Society*, 2022. <https://doi.org/10.1177/1461448221088274>; Demystifying Disinformation Shadow Economies: Fake News Work Models in Indonesia and the Philippines. Jonathan Corpus Ong and Ross Tapsell, *Asian Journal of Communication*, 2022. <https://doi.org/10.1080/01292986.2021.1971270>

19. Peddling Secrecy in a Climate of Distrust: Buzzers, Rumours and Implications for Indonesia's 2024 Elections. Yatus Sastramidjaja, Pradipa P. Rasidi and Gita N. Elsitra. *ISEAS Perspective*, 24 August 2022. <https://www.iseas.edu.sg/articles-commentaries/iseas-perspective/2022-85-peddling-secrecy-in-a-climate-of-distrust-buzzers-rumours-and-implications-for-indonesias-2024-elections-by-yatus-sastramidjaja-pradipa-p-rasidi-and-gita-n-elsitra/>; Buka-bukaan soal Buzzer (1): Pengakuan Denny Siregar dan Pehip Nugraha soal Buzzer Istana. Nibras Nada Nailufar, *Kompas.com*, 9 October 2019. <https://www.kompas.com/tren/read/2019/10/09/060029265/buka-bukaan-soal-buzzer-1-pengakuan-denny-siregar-dan-pehip-nugraha-soal?page=all>

20. Southeast Asia's Troubling Elections: Nondemocratic Pluralism in Indonesia. Edward Aspinall and Marcus Mietzner, *Journal of Democracy*, October 2019. <https://doi.org/10.1353/jod.2019.0055>; Cyber Mercenaries vs the KPK. Wijayanto and Albanik Maizar, *Inside Indonesia*, 13 October 2021. <https://www.insideindonesia.org/editions/edition-146-oct-dec-2021/cyber-mercenaries-versus-the-kpk>

21. It should be noted that, although Jokowi has been a major beneficiary, Prabowo and other political elites have likewise employed their own influence operators.

22. Transformative Working-Class Labor in Indonesia's Political Influence Operations. Pradipa P. Rasidi, *Influence Industry Explorer*, 31 October 2023. <https://influenceindustry.org/en/explorer/case-studies/indonesia-political-influence-operations/>

23. Inside Indonesia's New Communications Agency: Shaping President Prabowo's Message. Mochamad Azhar, *GovInsider*, 14 May 2025. <https://govinsider.asia/indo-id/article/inside-indonesias-new-communications-agency-shaping-president-prabowos-message>

24. Transformative Working-Class Labor in Indonesia's Political Influence Operations. Pradipa P. Rasidi, *The Influence Industry Project*, 31 October 2023. <https://influenceindustry.org/en/explorer/case-studies/indonesia-political-influence-operations/>

25. Aktivisme Digital di Indonesia. Muhammad Fajar, Aulia Nastiti, Yoes C. Kenawas and Luthfi Adam, Yayasan Tifa, 2022. <https://www.tifafoundation.id/buku/aktivisme-digital-di-indonesia/>; Global Perspectives on NGO Communication for Social Change. Edited by Giuliana Sorce, Routledge, 2021. <https://doi.org/10.4324/9781003188636>.



LISTENING CIRCLE

A space to pause, reflect and breathe

In the midst of all the chaos, uncertainty, and relentless change swirling through the media industry right now, Sanne Breimer and Mili Semlani host a virtual community-led, safe space every month.

We gather to witness, support, and hold space for whatever we're experiencing. Share what feels right in the moment, or simply listen.

RSVP

<https://lu.ma/k0ndv666>



Growing Sideways

The Seapunk imagination



Seapunk 'sloppy' concept art for S.N.O.W., a soon-to-be-released fictional world built around the themes of climate agency, distributed resilience and post-apocalyptic SMEs.

Sam de Silva, producer of *Balance*, and Sam Chua, founding curator of Seapunk Studios, discuss how imagination, fiction and decentralised design can open up new ways of thinking about power, technology and resistance.

Sam, you used to work within the digital rights and tech accountability movement. What made you step away from that space and start Seapunk?

▶ I was quite active in the space from about 2016 to 2020, when I worked closely with [Digital Asia Hub](#) and many adjacent actors. That gave me a lot of exposure — I learned about the dynamics of digital platforms, power imbalances and rights-based responses. But, over time, part of me also began to feel that the space as a whole tended to be reactive; defensive, even. And while that's necessary — we need people running interference, building shields, advocating for fair protections — I found myself drawn towards other, more generative directions, inspired in part by some of the experiments I had the chance to be part of with Digital Asia Hub: speculative fiction, summer schools, playshops, dolphin tanks — as opposed to “shark tanks” — and more.



What if, instead of focusing on and reacting to the latest harm, we spent more energy creating our own spaces and protecting them? Not in opposition, but with a kind of indifferent punk sensibility.

I started wondering: What if, instead of focusing on and reacting to the latest harm, we spent more energy creating our own spaces and protecting them? Not in opposition, but with a kind of indifferent punk sensibility. Not aggressive, but indifferently creative. Like punk music — it doesn't set out to destroy the mainstream. It just cuts a hole in the fence and finds its own space to play.

That's the energy I wanted to explore with Seapunk. Not confronting some villainous Big Tech figure, but building worlds that don't depend on the villain at all. We still care about fairness, justice and power, but we're more interested in the deeper question: What are rights for? What kind of life do they serve? And can we think beyond the conventional confrontational dialectic to get there?

Can you unpack the name Seapunk for us?

▶ Seapunk works on a few different layers. First, as a genre label — like solarpunk, cyberpunk, steampunk. These are all aesthetic orientations or speculative traditions. Solarpunk is about hopeful ecological futures. Cyberpunk is about high-tech dystopias. Seapunk is our exploration of Southeast Asian experimental solarpunk-inspired futures.

Why "Seapunk"? There's "SEA", as in Southeast Asia. But also "sea" as in water — the sea as a medium that shaped so much of this region's history; that carried trade, culture, migration; that allowed for a kind of decentralised coherence, where distant places could be networked without being unified under a single empire. That's a big part of the punk spirit too — autonomy without isolation.

And then there's the idea of "Option C" or a third way (in the original self-declared coining of "Third World"). Not Superpower A or Superpower B. Not capitalist bloc versus communist bloc. "C" or "SEA" as a third way. Something more non-aligned, fluid, peer-to-peer. That idea of another way that's cooperative, decentralised and rooted in local agency. That runs through a lot of what we do.

You recently ran the Seapunk Midsummer Studio in Chiang Mai. Can you tell us what that looked like in practice?

▶ The Seapunk Midsummer Studio, or SMS, was a [ten-day gathering](#) of a couple dozen people — about half traveling participants and half folks who were already in Chiang Mai. It was designed as an open-ended container. We had reading seminars, fiction jams, design sessions and an academic paper presentation. We also spent a lot of time sitting around, talking, sketching, thinking, researching, imagining.

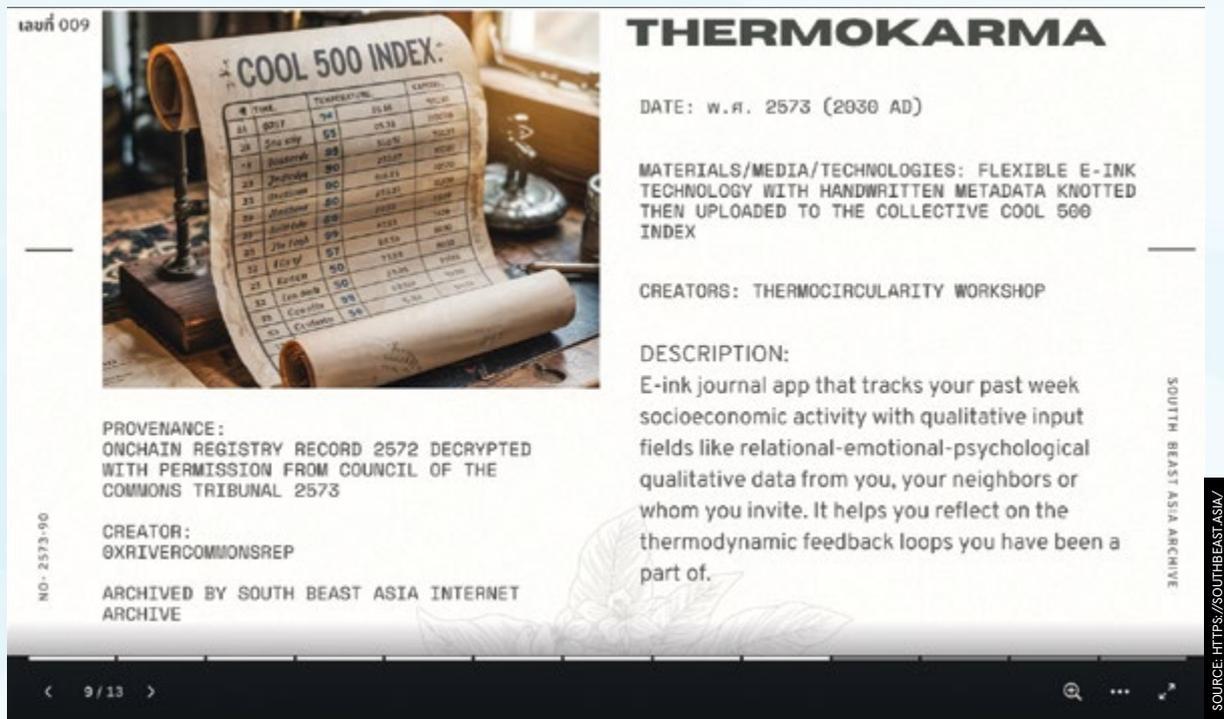
One activity was a sci-fi workshop called 'Good Ghosting'. We explored the idea of artificial ghosts — AIs programmed to inhabit objects or places. So instead of AI as an all-knowing chatbot, we imagined small, localised presences: artificial ghosts. A ghost in a tree. A ghost in a temple gate. A ghost in a marketplace stall. These ghosts might monitor soil health, protect a forest, tell stories or mediate conflicts. They don't scale. They haunt. And they nudge us to ask: What does it mean to embed intelligence into the world, not just on top of it?

We weren't trying to invent tech products. We were trying to loosen our thinking — to imagine technology as presence, spirit or kin. That kind of sideways approach led us to insights that straight-line policy work might otherwise have missed.

You also presented a paper on "imaginary decolonisation". What was that about?

▶ We presented at an academic conference on decolonising Southeast Asian studies. Our paper, co-authored by Jules Yim and myself, was titled 'Imaginary Decolonisation'. The idea is that real decolonisation doesn't stop at territory or institutions. It has to include, or even begin with, the imagination — how we see ourselves, what we think is possible, what futures we believe we're allowed to build.

If the powerful people in a postcolonial country still extract resources and exploit the land using colonial logics, that's not real decolonisation. Even if they look like us. Even if they speak our language.



An artifact from the archive gallery of thirteen South Beast Asia artifacts

We proposed four shifts: from dominion over nature to living with it, from centralised sovereignty to distributed sovereignty powered by shared commons, from either/or science and spirituality to a syncretisation of both, and from urbanisation-centric modernisation to cosmo-local reimaginings of rural versus urban ways of how we live upon the land. These aren't policies per se, although they underlie many potential policies and systems. They're orientations — prompts for imagining otherwise.

In the digital rights struggle, there's a lot of energy invested in trying to shift the needle on tech power, but it feels like we're always behind. What's your take?

► That's fair, I certainly feel that. And I don't have a five-point plan to fix it. But one thread we explored recently was thinking about AI through the lens of theology. The dominant public conception of AI feels very monotheistic. There's one AI behind an interface, whose behaviour we struggle desperately to align. You prompt it with some combination of words, almost like a prayer. It answers. It's mysterious and powerful, and generally speaks as though it's all-knowing.

But in one of our worldbuilding exercises earlier this year, what emerged was a universe of AIs that could best be described as wildly polytheistic. Where AIs are embedded everywhere — in trees, in cats, in altars. Small gods. Local intelligences. A distributed spiritual ecology.

That kind of model — a polytheistic model — enacts (or emerges) alignment through ecological checks and balances. Not through legislation or regulation, but through ecology. No single AI has all the power, just as in polytheistic pantheons, where no single god has all the power. They contradict each other. They protect different things. And the system becomes more resilient. Alignment, we discovered through this exercise, has different pathways. What if distributing agency could be just as, or perhaps even more, effective towards achieving dynamic societal balance as fighting for rights?

That idea has stayed with me. What if balance in tech didn't always come from one big governance structure, but from cultivating many small, overlapping agents? That's not something I learned from a digital rights report. It came from imagining sideways.



Not confronting some villainous Big Tech figure, but building worlds that don't depend on the villain at all.

So is Seapunk trying to build these systems? Or just imagine them?

► Seapunk Studios is mostly upstream, at the level of culture and imaginaries. We do research and imagination. But much of what we produce might also filter and manifest downstream. Some builders or policymakers or social entrepreneurs might encounter these provocations, these patterns, and apply them to their work — whether in cybersecurity, design, education, policy or otherwise. So Seapunk is about expanding the imagination layer, which in turn expands all downstream layers from there, which we hope expands the range of futures we might build and inhabit.

We're not just imagining by ourselves, but also creating and sharing scaffolding for others. For example, we created a tool called the [Protocol Design Fiction Canvas](#) for a workshop earlier this year. It's a way to build imagined worlds through designing their component artifacts, systems and protocols. This is what we more or less used in the building of [South Beast Asia](#) earlier this year. It's now released for groups and facilitators to use under a Creative Commons license. Anyone can use it. Some already have.

I'm personally interested in taking certain concepts further — maybe into apps or prototypes. But I don't think everything needs to scale, and certainly not led by me or with myself as the bottleneck. Sometimes fertilising the field is enough.

How do you see this connecting with civil society organisations more broadly?

► I don't think we're trying to convince or convert anyone, civil society organisations, corporations, entrepreneurs and so forth. Punk doesn't try to fix others. It makes the things it's interested in and leaves the door open.

We host and run playshops. We publish tools. We jam with people who are curious. Some of those people are policymakers. Others are artists or engineers. And when they remix what we've done in their own context, that's great.

One of the benefits of fiction and speculation is that it lets you break out of the "solution space". You don't have to fix the world. You just ask what other worlds are possible — and maybe fun.

Are you hopeful this kind of orientation can actually rebalance power?

► Hope's a funny word. But I'm energised.

At the end of the Midsummer Studio, we held a salon on power. Some people felt overwhelmed — that Big Tech is too entrenched and people are powerless. But someone said, "Power is just one lens. There's always agency, if you shift the frame."

That stuck with me. Even a seed growing out of the side of a cliff isn't thinking about power. It just notices water in the crack, finds light, and grows.

That's how I think about Seapunk. Not trying to solve a huge systemic problem, but learning how to grow sideways. To sense. To relate differently to complexity. And what's been encouraging is that other people — even some system designers — have felt energised by that too.

Not everyone building big systems wants to dominate. Many are looking for ways to design without bottlenecks and move past extractive or parasitical dynamics. So if our weird little imaginings can offer tools, moods or metaphors that help — that's already a win. 📦

BIOS:

Sam Chua is a cultural entrepreneur and the founding curator at Seapunk Studios. His work explores the intersections of research, imagination, and the catalytic hosted experience.

Sam de Silva is the founder and producer of Balance and lead of CommonEdge Asia. He works at the overlaps of technology, culture, human rights and info/communications.



COMMON EDGE

***CommonEdge Asia* offers a range of services that bridge insight, action, and innovation.**

We work with partners to navigate complexity, design strategic responses, and shape digital futures grounded in justice, accountability, and care.

Our offerings include:

- > Tech Design and Development
 - > Digital Literacy and Education
 - > Strategic Advisory Services
 - > Communications
 - > Digital Safety and Security
- and much more...



Visit <https://commonedge.asia> for more or contact us at info@commonedge.asia

Index to URLs



Designed for Control
Infrastructure, Power and the Public



Power Plays
The uncomfortable position between governments and tech companies



Who Writes the Rules?
The new order of platform power



From Recruitment to Resistance
When it comes to fighting radicalisation, fixing the tech is only one piece of the puzzle



"Show Us Your Screens"
Algrave and the radical joy of live coding



Platform Power and Populism:
The architecture behind Hindu nationalism's digital rise



A Just Transition to an AI Future
Pursuing a labour-first AI agenda



Documenting Resistance, Building Alternatives
The App Censorship Project and the struggle for digital freedom in Asia



Navigating the Labyrinth
Finding community on social media



Campaigns, Clicks, and Complicity
How civil society actors built the 'buzzer' industry



Resisting Oppression
Focusing on information needs



Growing Sideways
The Seapunk imagination



Networks and Minefields
When social media presents both opportunity and risk

