EngageMedia

Pandemic of Control:

COVID-19 and the Rise of Digital Authoritarianism in the Asia-Pacific

In partnership with

COMMON EDGE

EngageMedia is a nonprofit that promotes digital rights, open and secure technology, and social issue documentary. Combining video, technology, knowledge, and networks, we support Asia-Pacific and global changemakers advocating for human rights, democracy, and the environment. In collaboration with diverse networks and communities, we defend and advance digital rights.

CommonEdge is a platform for projects that responds to digital/tech power. We do this by understanding the digital world around us and sharing our findings, and collaborating and implementing initiatives that address specific issues related to the digital world.

Published September 2022

ISBN 978-0-9873977-1-3

Table of Contents

COVID-19 has dramatically accelerated the authoritarian use of digital technologies. Digital surveillance has radically increased, with governments tightly tracking the movements and associations of their citizens. Physical spaces became digitally gated – from cafes and libraries to even whole countries – with ordinary citizens recruited to ensure compliance. In-sync, unsecured databases have become bloated with more and more personal health information.

To manage the pandemic, governments and other vested stakeholders have unleashed their own pandemic of control. Officials, medical experts, the mainstream media, and Big Tech pushed the narrative that COVID-19 could be tightly controlled, and that citizens everywhere had a responsibility to abide, with no questions asked, to achieve that aim.

The "approved" pandemic response was defended at all costs. News media ridiculed alternative viewpoints as fake news and misinformation, and social media platforms took down contradictory views from their feeds, silencing voices that questioned vaccine passports, lockdowns, and other controls.

And while restrictions continue to be eased in most countries, in others they are not. In addition, much of the infrastructure remains at the ready, and the population itself is now well-groomed for the new sets of demands, from digital IDs to central bank digital currencies and beyond.

The pandemic is not yet over, but a new chapter has begun, one with more space for the digital rights community (which has been unusually quiet throughout), journalists, and the wider public to question this pandemic of control.

Questions could include why governments released check-in apps prone to data breaches, or how fact-checkers and content moderators reportedly worked with digital platforms to remove information that has since been confirmed or, at the very least, worthy of further investigation. For example, why was the hashtag #naturalimmunity considered so dangerous that it had to be censored by Instagram? The Centers for Disease Control and Prevention recently updated its guidelines to acknowledge the protective value of prior infection. Why was discussion of this previously disallowed? Where were the progressive voices of opposition, the voices that question power?

Most concerning is a general trend among citizens, including progressives, to sacrifice civil liberties and free speech and expression in favour of an authoritarian and top-down, "trust the experts" model. This has resulted in a lack of accountability for government and corporate leaders (for example, the former Australian Prime Minister appointing himself secretly to 5 ministries), protecting the powerful from scrutiny that might have resulted in better solutions for society as a whole.

To generate further public discourse, EngageMedia in partnership with CommonEdge invited writers, researchers, and changemakers in the Asia-Pacific to respond to the growing digital authoritarianism accelerated by COVID-19 and the absence of critical questioning.

The result is the Pandemic of Control series, a modest contribution toward a more critical citizenry. In this collection, you will find pieces from Indonesia, Vietnam, India, Sri Lanka, Bangladesh, Nepal, and Australia. The authors question the how and the why of their respective countries' pandemic response, and shed light on more rights-respecting paths moving forward.

This digital reader includes 10 pieces that were published between April and August 2022. We felt it was important to create this compilation so the responses to the pandemic-driven digital authoritarianism be distributed more effectively as a collection.

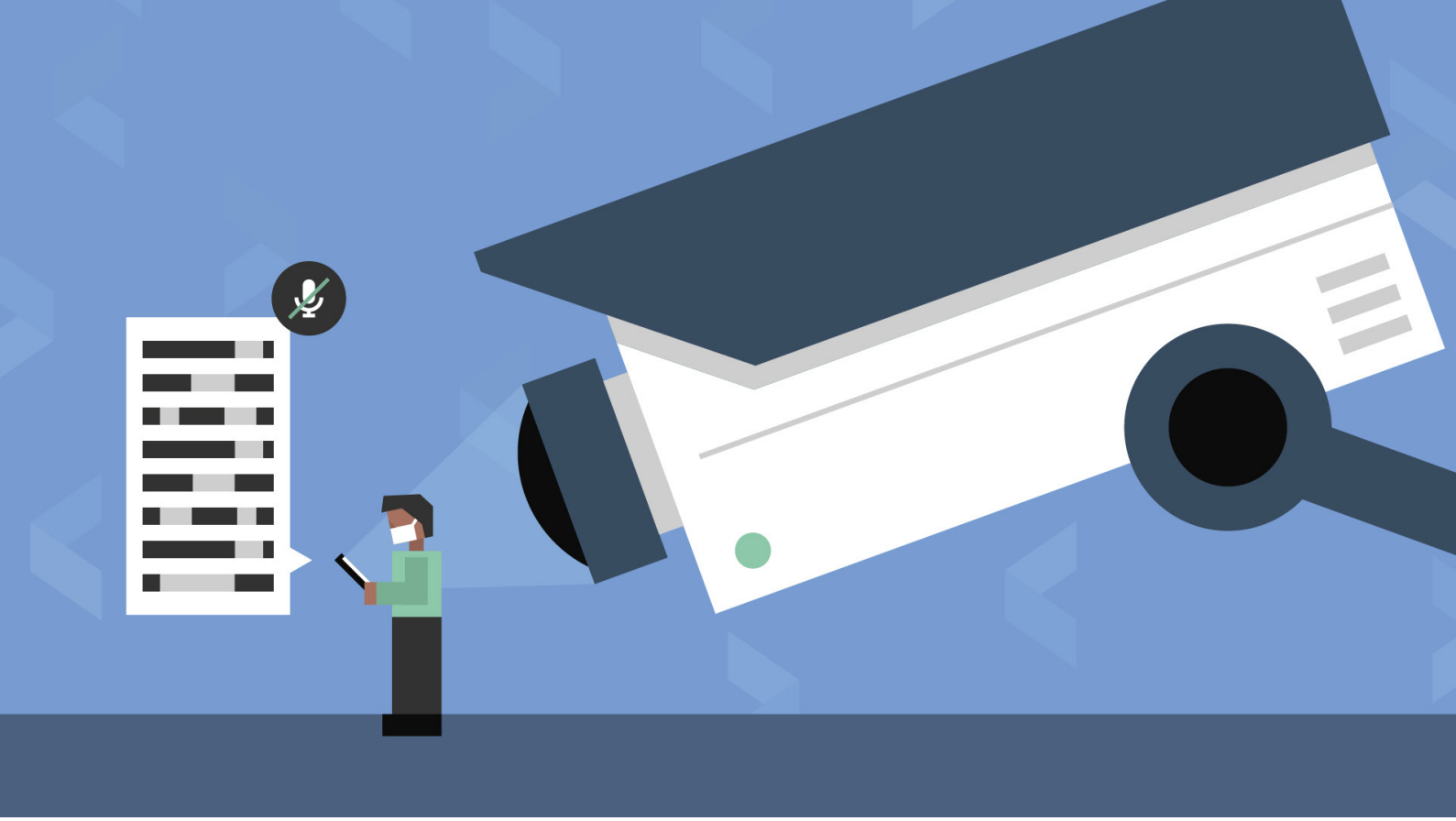
We plan to publish 6 more articles between October and December 2022, and these pieces will be added to a second edition of the Pandemic of Control digital reader.

If you are interested to engage further with the authors, EngageMedia, or CommonEdge, you may contact us through our website.

Thank you,

Andrew Lowenthal, Executive Director, EngageMedia

Sam de Silva, CEO, CommonEdge



Digital authoritarianism in Bangladesh: Weaponising a draconian law to silence dissent in the pandemic era

ZAYED SIDDIKI

In the past decade under the current administration, Bangladesh has seen not only digitalisation and economic growth, but also a worsening human rights situation and growing authoritarianism. Reporters Without Borders describes the current government as "more authoritarian and ready to crack down on press freedom". With critics muzzled, there is currently no effective political opposition in the country, reflecting Bangladesh's long-standing struggle to sustain a fragile democracy since independence in 1971.

The COVID-19 pandemic has only exacerbated the administration's increasingly authoritarian agenda. Lockdown measures were implemented unequally, with movement restrictions strictly enforced against political opponents and the general public. Authorities introduced movement passes that posed risks to people's privacy and data security. A controversial law was weaponised to stifle criticism of the government's handling of the health crisis.

During the early days of the pandemic, citizens became vocal on social and mainstream media about the government's ineffective response and the corruption of ruling party leaders. People criticised the delayed and unequal application of lockdown rules to restrict physical mobility, corruption in the purchase of protective health gear, the embezzlement of relief packages, and the low rates of testing and lack of information on case detection.

These issues created a huge controversy. Except for a few arrests of local leaders linked to corruption, the government's response was to go after anyone criticising the pandemic response. It fiercely applied legal instruments against journalists, academics, ordinary citizens, and even government officials and doctors speaking out about these issues. An oppressive law, the Digital Security Act (DSA), was used to pick out and punish these dissenting voices.

Using the Digital Security Act to silence dissent

Before the DSA came into force, freedom of expression in Bangladesh was already under attack through the Information and Communication Technology (ICT) Act. Passed in 2006, the law contains the controversial Section 57, which authorises the prosecution of anyone who publishes electronic material deemed fake, obscene, defamatory, or that "tends to deprave or corrupt" its audience. Civil society and human rights organisations have said that Section 57, and the other vaguely-defined provisions in the law, tightens the noose on free speech on digital platforms.

The DSA was passed in 2018, replacing the ICT Act. But the DSA is considered more repressive and draconian in nature than the law it replaced, and is deeply problematic for three broad reasons:

1. Vague sections of the law that may lead to criminalising legitimate expression of thought or opinion;
2. Broad powers granted to authorities – such as the power to arrest people and search premises without a warrant, requiring only the suspicion that a crime was committed using digital media;
3. Provisions which allow for the removal or blocking of content and the seizure and search of devices without sufficient safeguards.

From 2012 to 2020, around 2,000 cases have been filed under the ICT Act and the DSA. Of these, only 2 percent ever led to convictions, suggesting that the law has been used more as an instrument to harass citizens and dissenting voices.

ARTICLE 19 raised the alarm over the increasing number of charges and arrests made under the DSA based on social media comments. According to an April 2022 report by the Centre for Governance Studies, at least 2,244 individuals were accused of violating the DSA between January 2020 and February 2022. During this period, 842 people were arrested. Most striking in the report was the clear indication that members of the ruling party were using the DSA to target the media and political opponents. Of those accused whose professions are known, 30.98 percent were politicians, and more than a quarter were journalists.

The pandemic saw the surgical use of the DSA against journalists and critical voices pointing out inefficiencies in the government's health response, problems in the distribution of aid, and vaccination irregularities. Citizens from all walks of life were also targeted, including a 15-year old boy who criticised the Prime Minister on social media. Other notable cases include:

- The arrest and torture of cartoonist Ahmed Kabir Kishore, who was detained in May 2020 over a series of images titled "Life in the Time of Corona", published on Facebook. The cartoons were a satire of the government's pandemic response. Kishore was released in March 2021 after 10 months in detention. On his release, he was unable to walk and was mentally devastated. He also complained that he was denied medical treatment in jail.
- The arrest and custodial death of writer Mushtaq Ahmed is the most notorious; he was arrested in May 2020 for allegedly spreading misinformation about the pandemic. During his detention he was reportedly tortured before he passed away in February 2021.
- Minhaz Mannan Emon, director of the Dhaka Stock Exchange, and Didarul Bhuiyan, activist and coordinator of the Facebook page 'Rashtrachinta' (Thoughts on the State), were arrested for spreading alleged rumours on the government's handling of the pandemic. They were accused of tarnishing the image of the state and the country's founding president. However, there were no specific charges against Minhaz. According to the charge sheet, Minhaz was found to have privately chatted with one of the accused on WhatsApp and Facebook Messenger, although there were no details of the conversation between them.

As a result, the DSA has also cultivated a culture of fear and self-censorship among citizens. Civil society members, journalists, political activists, and ordinary citizens are now forced to think twice before writing or making comments online. There have

been several protests and activist actions calling to abolish the draconian law, but the government has not acted on these calls.

Mass surveillance using movement passes and big data collection

Aside from the DSA, another tool in the government's increasingly authoritarian agenda is an attempt to monitor citizens' movements. In April 2021, the Bangladesh police launched a 'Movement Pass' application which would allow outside movement during the strict lockdowns imposed at the time. To register, one needed to use the app or visit movementpass.police.gov.bd and provide a cell phone number, name, birth date, date and time of movement, photographs, and identification cards. A person was allowed a maximum of five passes a day for emergency trips such as going to the hospital, purchasing medicines, and grocery shopping.

In the first five days of implementation, over 600,000 passes were issued. The passes needed to be shown before checkpoints; failing to provide a pass resulted in on-the-spot fines and punishment such as detention and imprisonment. The system prompted confusion and chaos, and hundreds were fined and arrested for breaching lockdown rules. It also created controversy as those who did not have smartphones or an internet connection could not apply for the passes. The implementation of lockdown rules also varied, as ordinary citizens faced strict restrictions, while those supportive of the government were given an advantage.

This kind of data collection has major implications for digital rights. In a media report, information technology expert Sumon Ahmed Sabir flagged the risk of mass surveillance through the collected data – a risk heightened even more if a third party could access the data. Additionally, Supreme Court lawyer Jyotirmoy Barua pointed out that the police did not have the jurisdiction to control people's movements, and that the system only served to advance the mass surveillance process.

There is also no law in Bangladesh to protect personal data, although a Data Protection Act is currently being drafted. However, this has also been a point of controversy. Analysts have pointed out that the draft law contains loopholes which, instead of protecting citizens, may further suppress digital rights especially when there is already a culture of mass surveillance by the state.

The movement pass system was abolished during the second strict lockdown in July 2021. But concerns remain over the country's democratic regression and the weaponisation of laws to curtail people's rights and freedoms. As these cases have shown, the pandemic provided the government with pretext to censor free speech,

harass critics, and effectively curb dissent – accelerating what has been an ongoing turn towards authoritarianism in Bangladesh.

Zayed Siddiki *is an award-winning independent filmmaker, human rights defender, and development communications professional based in Dhaka. His area of work includes right to information and communication justice, good governance and transparency, privacy rights and data protection, and freedom of expression, among others. He holds two post-graduate degrees: one in Television and Film Studies from the University of Dhaka and another in Graphic Communication from Loughborough University.*

A COVID-19 power grab: Looming digital authoritarianism in Indonesia

DAMAR JUNIARTO

Read this post in Bahasa Indonesia

In Indonesia, a multi-ethnic country of 270 million citizens, a rise in hard-line approaches to governance is heralding a looming authoritarianism. The COVID-19 pandemic provided the Indonesian government with the opportunity to accelerate digital authoritarianism, invoking the spectre of "guarding national security" and "creating stability during the COVID-19 pandemic".

In 2020, Indonesia ranked 64 with a score of 6.30 in The Economist Intelligence Unit's Democracy Index, putting it into the "flawed democracy" category. While the 2021

index showed the country improving to rank 52, there are still significant obstacles for the exercise of democracy. Various reports from Freedom House, IDEA, and Reporters Without Borders, for example, highlighted the problem of shrinking civic spaces, both on and offline. Several national reports have come to the same conclusion: in 2020, a survey by the Indonesian National Human Rights Commission showed 29.4 percent of Indonesians felt they were not free in expressing criticism of the government. Meanwhile, 52.1 percent of respondents in an April 2021 survey conducted by LP3ES and published in Tempo.co (which caters mostly to the urban middle and upper class) said they were afraid to express their opinions and form associations.

The number of internet users In Indonesia is now 204.7 million as of January 2022, representing 73.7 percent of the total population. As more of public life goes online, so do government attempts to restrict people's rights and freedoms.

A COVID-19 power-grab

I head the Southeast Asia Freedom of Expression Network (SAFENet), a regional organisation focused on promoting and protecting digital rights in Southeast Asian countries. In 2020, we released a report titled "The Rise of Digital Authoritarianism", which recognised democratic regression in Indonesia.

Alina Polyakova, president of the Center for European Policy Analysis, and Chris Meserole, Director of Research at the Artificial Intelligence and Emerging Technology Initiative, define digital authoritarianism as "the use of digital information technology by authoritarian regimes to surveil, repress, and manipulate domestic and foreign populations". Since 2019, Indonesia has seen an acceleration in the indicators of digital authoritarianism: online censorship, cyber surveillance, and internet shutdowns.

Online surveillance

When the pandemic hit Indonesia in March 2020, President Jokowi instructed state intelligence bodies to ensure public order to quell public fears and panic. A month later, police started to actively control narratives about the COVID-19 situation in the country, especially on social media. For example, on April 4, 2020, the National Police Headquarters issued Telegram Letter No. ST/1100/IV/HUK.7.1/2020, which instructed the police to carry out cyber patrols to monitor online opinions and to take action against those spreading hoaxes about the pandemic, government policies, and those insulting the President and the government. Amnesty International reported that at least 57 people were arrested for spreading "false news".

In February 2021, the government rolled out a "virtual police" that would patrol online platforms to monitor content posted by citizens, with an intended aim of reducing crime related to the Electronic Information and Transaction (ITE) Law. With this setup, police

had the power to send virtual alerts directly to social media users, warning them and ordering them to delete posts deemed unlawful. Between February to March 2021, the virtual police had sent out warnings to 89 social media accounts for spreading content tagged as hate speech. This virtual police creates a new fear that limits privacy and freedom of expression for Indonesians.

The PeduliLindungi app, launched during the start of the pandemic, has also posed privacy and digital security concerns. Initiated by Indonesia's Ministry of Communication and Information Technology (MCIT) and the Ministry of State-Owned Enterprises (MSOE), it was designed to track people's exposure to COVID-19. Audits conducted by DigitalReach and CitizenLab flagged several privacy issues with the application, particularly regarding excessive permissions and unnecessary features. For instance, in its 2020 report, CitizenLab noted that the app collects users' WIFI MAC addresses and local IP addresses, which can help identify users and are not necessary for contact tracing. The app also sends the device's location information and user info to the developers' servers, allowing them to track the physical locations of the devices.

In its 2021 Indonesia report on human rights practices, the US Department of State noted "NGO concerns about what information was gathered by the application and how this data was stored and used by the [Indonesian] government" under a subsection on unlawful interference with privacy. While the Indonesian government asserted that measures have been taken to address security concerns in the app, concerns remain on the data security of users. The application was also extended for vaccine certificates and then as a system of digital gating, denying access to the unvaccinated to malls, shops, and other locations. There are unresolved questions on who owns the users' data.

Online repression

The pandemic provided law enforcement officers with an opportunity to employ the ITE law to exert excessive restrictions on freedom of expression. The law, which aimed to prosecute cybercriminals, contains several provisions that expand the government's power to punish social media commentary. Under this draconian law, activists using their social media accounts to express dissent may face criminal charges related to hate speech, online defamation, or even treason, as in the case of Papuan activists.

The ITE law has become a weapon used by the state to silence critics, although it is also widely used by politicians and businessmen against their critics. It is increasingly used against ordinary citizens, activists, and journalists, especially those investigating environmental and human rights violations. The number of charges filed under the ITE Law's defamation clause has increased: from 24 in 2012 to 84 in 2020, and 91 in 2021. Some of these charges stemmed from criticism of the government's COVID-19 response. In September 2021, for instance, the Presidential Chief of Staff filed defamation accusations against two Indonesia Corruption Watch researchers over a

study that they conducted. The study alleged that various government officials were involved in promoting the use of the drug Ivermectin during the pandemic.

Meanwhile, attacks using sophisticated digital technology have also been used as a form of online repression. The National Human Rights Commission (Komnas HAM) said that between 2020 and 2021, they received reports of hacking incidents against critical media, organisations, and individuals – all while the pandemic had been impacting the country. One such case was that of researcher Ravio Patra, a critic of the government's pandemic response. He was arrested for allegedly broadcasting a message that "incites hate and violence", but rights groups maintain that his account had been hacked. There have also been similar incidents against online media tirto.id, in which an unknown hacker removed news articles critical of the Indonesian intelligence agency's role in the pandemic response.

Technological oppression in the form of digital attacks is getting worse. According to a SAFEnet digital rights situation report in 2020, at least 147 digital attacks occurred in 2020 alone. Almost all of these digital attack cases were related to those who criticised government policies on various issues, particularly the pandemic response. In 2021, the number of digital attacks rose to 193, with an average of 12 incidents per month.

Online manipulation

A report by Diponegoro University revealed the Indonesian government's use of cyber mercenaries (locally known as 'buzzers') to raise support for controversial policies amid the COVID-19 pandemic.

This manipulation was conducted by buzzers, fluid networks of sockpuppet accounts, influencers, content creators, and political consultants who work together to orchestrate public opinion on social media by creating a particular narrative on certain political issues. Cyber mercenaries are typically funded by politicians, political parties, and business people. These cyber mercenaries operate by spreading hoaxes, disinformation, doxing, and trolling.

During the height of the COVID-19 crisis, these cyber troops were deployed to rally public support for the government's New Normal policy, which urged citizens to carry on with their normal activities while observing health protocols. In June 2020, several local governments and civil society groups pushed for lockdowns to curb transmissions. In response, a number of central government agencies solicited influencers for the New Normal campaign to promote economic recovery. Their strategies involved amplifying news reports – mostly from media outlets owned by media moguls cum ruling party politicians — that underplayed the deadliness of COVID-19, as well as harassing and doxing critics of the government's pandemic mismanagement. The aim of this combined deployment of sockpuppet accounts and influencers was two-fold: to promote a singular national narrative that COVID-19 was not a deadly crisis, while also deterring opposition from civil society and local government actors with dissenting policies.

These strategies have been successful in co-opting the Indonesian digital public sphere and preventing it from becoming a free space where the voices of civil society can be heard. In this regard, the online public opinion manipulation by cyber mercenaries can be seen as one of the most significant signs of the rise of digital authoritarianism in Indonesia.

Civil society in Indonesia needs to push back against this democratic regression to prevent the country from falling into the abyss of authoritarianism.

Damar Juniarto *is a human rights activist known for his work on digital rights and online freedom of expression in Southeast Asia. Since 2013, he has been the Executive Director of Southeast Asia Freedom of Expression Network (SAFEnet). He also serves as Advisor at DigitalReach, a regional organisation that looks into the impact of technology on human rights in Southeast Asia. Damar has received accolades for his work, including recognition as one of Rest of World's Global Tech Changemakers in 2022 and the Anugerah Dewan Pers (Indonesia's Press Council Award) for promoting press freedom in Indonesia.*

Policing the pandemic: Australia's technology response to COVID-19

SAMANTHA FLOREANI

In early 2020, COVID-19 took hold in Australia. We watched as the lockdowns in Wuhan, China became more commonplace, and the virus made its way across the world. In Australia, the government policy evolved to become 'zero COVID', enforced through the donning of masks, social distancing, and oftentimes, lockdowns. Suddenly, almost every aspect of our lives moved online.

In times of crisis, governments often rush through additional powers, many of which put human rights at risk, and are rarely wound back once we return to relative calm. The ubiquitous technologies of the digital age, combined with a pandemic requiring us to isolate ourselves from each other, tilled the soil for a future where digital surveillance and control could bloom. In anticipation of this, human rights advocates urged governments to uphold human rights in any technological response to COVID-19. As

lawyer and digital rights activist Lizzie O'Shea puts it: "What will get us through this virus is not coercion and fear, but advocating for and carrying out the politics of care and solidarity".

Digital technologies can play an important role in supporting a robust public health response. The question is not if we should use technology, but how. The technological choices made by Australia's state and federal governments during this tumultuous time speak volumes about their priorities and ideologies. By reflecting on the past two years, we can observe a trend: rather than employing technologies to improve and enhance care and support of the population they were responsible for, governments in Australia prioritised politically buzzworthy projects based on an ideology of surveillance and control.

In this piece, we examine four technology-based government responses to the COVID-19 pandemic: police use of drones and other mobile surveillance cameras, the COVIDSafe App, the QR code check-in system, and facial recognition-enabled home quarantine apps. These, coupled with avoiding transparency and a reluctance to engage with technical experts and civil society, ultimately resulted in technological "solutions" that ranged from outright ineffective to actively punitive.

Over a period of more than two years, these rules and policies combined to create an environment where those in Australia were left without work, with inconsistent support, and the threat of punishment for transgressions by law enforcement with beefed-up powers. Many struggled with frequently changing rules that conveyed confusing or conflicting instructions. Vital health advice was often not sufficiently translated into languages other than English. On top of this:

- Most states across Australia declared a state of emergency and brought in new laws that imposed severe restrictions on civil liberties and an increase in policing powers.
- Individuals could face significant fines if caught breaching a pandemic order or direction (such as lockdown restrictions). For example, individuals could be fined up to 10,904 AUD in Victoria and up to 11,000 AUD in New South Wales (NSW). In Victoria, which endured the longest duration of severe lockdown restrictions, disadvantaged communities were disproportionately impacted by fines.
- Australia adopted hardline international border control policies that restricted individuals from travelling into or out of the country. Even Australian citizens were not able to go home. Many individual states also adopted similar controls on their internal borders.

It is in this landscape that many individuals and communities were left scrambling, forced to turn to each other for mutual aid, and in many cases, risk breaking lockdown rules in order to survive.

Police drones and mobile surveillance

In late 2020, Australian media outlets reported that Victoria and NSW Police were using drones to monitor and enforce COVID-19 rules in public spaces including parks and beaches. This created significant unease among the public about surveillance capacities, to which Victoria Police attempted to publicly reassure people. Alongside this, mobile camera surveillance units were deployed throughout parks and other public spaces, and CCTV was repurposed to police COVID-19 restrictions, to the public's dismay and anger. Many criticised the government's aggressive and punitive approach to monitoring and fining individuals breaking lockdown rules, and expressed concern that governments and law enforcement were overstepping their authority without adequate safeguards, transparency, or accountability requirements.

Contact tracing and the COVIDSafe app

In April 2020, the federal government released its solution to the challenge of contact tracing: the COVIDSafe App. It was accompanied with a swathe of political rhetoric to convince people to download it. We heard moralising wartime metaphors, claims that the app would offer protection from infection "like sunscreen", and patriotic calls to join "Team Australia". The Australian public was told that 40 percent uptake was needed—a number which, it would later be revealed, was based on nothing. Over 7 million people downloaded the app, but widespread distrust of the government's technical ability, mishandling of privacy and security concerns, and technical flaws in the app's design all contributed to downloads never reaching the made-up target.

The app was designed to use Bluetooth to detect and record unique identifiers of nearby phones, provided they were also using the app. If a person tested COVID-19 positive, the list of all those they came into contact with was sent to the government, which then notified those who may be at risk. Crucially, it was found that the app did not work unless it remained open. This was a fundamental flaw, as it was impractical to have it open at all times.

Another key concern was the app's *centralised* model, which required the government to act as the middleman and to handle all the personal information collected. While contact tracing was accepted as useful and necessary to manage the spread of COVID-19, the potential for mass surveillance or other misuse of such revealing social interaction data was not underestimated. Privacy and security advocates strongly recommended the government take a decentralised approach, in which people's phones would directly alert others should they be exposed to the virus, without needing the government to act as a conduit. This was ignored.

In spite of this, digital rights advocates in Australia were successful in pushing the government to incorporate specific privacy protections into legislation governing the

app, including limitations preventing the use of the data for purposes other than public health.

Almost two years after the launch, a report evaluating the app's effectiveness showed that it did not add much value to the existing, conventional contact tracing system, and in some instances actually increased the workload of contact tracers. The app cost 7.7 million AUD to develop, and an additional 60,000 to 75,000 AUD per month to maintain. As of December 2021, the Australian government refuses to release data on how many people continue to use the app.

Notably, the federal government is now reportedly considering alternative uses of the app, presumably to save face after having spent so much time and money on something that turned out to be practically useless. It is not difficult to imagine how an app designed to track the interactions of individuals could be misused in a context other than contact tracing in a pandemic.

QR code check-in system

In November 2020, a new process to "check-in" to shops and venues using smartphones and QR codes arose. While this system would prove to be more useful than the COVIDSafe App for notifying people of possible exposure to the virus, this process was not without its challenges.

The rollout of the check-in system was chaotic. Each state established its own requirements, which varied drastically. In Victoria, for instance, the government initially made it compulsory for businesses to collect the personal details of individuals visiting their establishment, but this was not accompanied with guidance or support on how to do so safely. This resulted in many small businesses with little to no technical experience in security and privacy rushing to outsource their check-in requirements to third-party registration platforms. The personal information of millions of Australians was put at risk of being collected, used, and sold for purposes completely separate to public health, by a range of third party registration platforms—many of which are owned by companies whose primary business is dealing in data.

Eventually, state governments rolled out their own mechanisms for businesses to register for an official QR code to function with a government-run smartphone application. While this improved the initial problem, it did nothing to resolve the innumerable amount of people who had their details shared in the interim, and now receive marketing and spam text messages.

It also does not eliminate concerns regarding government bodies capturing and using data collected by way of the check-in system. On at least six occasions, police have

used check-in data for the purpose of law enforcement, a move condemned by the Australian Privacy Commissioner.

Home quarantine apps

In October 2021, the state of South Australia announced a trial of a home quarantine smartphone app. The app was designed to enforce compliance with home quarantine rules through geolocation and facial recognition software to confirm an individuals' identity and location at spontaneous intervals. Following the trial, other states around Australia also announced they would be trialling the app.

Technology experts, human rights lawyers, and civil society expressed concern regarding the use of such invasive technologies without strong privacy protections in place. Digital Rights Watch and Human Rights Law Centre wrote a joint letter to Australian health ministers, urging them to extend the same standard of legislative protections that were put in place for the COVIDSafe App to any other technological response to COVID-19.

Conclusion

Despite clear calls for assistance from affected communities for increased support, welfare payments, and funding for health services, governments prioritised responses that emphasised a punitive, surveillance-based approach. In doing so, Australian governments mistreated the social licence—the informal authority granted to the government by the people based on trust and confidence to see us through a major health crisis—for their own political agenda.

Looking back after two years, it is not clear that these approaches, nor the concessions given on civil liberties, were worth it or even effective. It is, of course, easy to say what should have been done with the gift of hindsight. Nonetheless, it is clear that Australian governments approached the use of digital technologies over the course of the COVID-19 pandemic from an ideological perspective, heavily leaning on control and surveillance and sidelining a politics of care and support.

Throughout the pandemic, technology experts, human rights organisations, and civil society groups in Australia have been loudly calling for governments to listen to their suggestions and consider their warnings. By ignoring them, federal and state governments missed an opportunity to build a robust and engaged multi-stakeholder response to COVID-19, and made many avoidable mistakes.

The COVID-19 pandemic is unlikely to be the only crisis that we face in our lifetimes, and it is important that we learn from this experience so that we can use digital

technology to respond in a more effective and rights-respecting way in the future. Just as advocates warned at the beginning of 2020, embedding human rights into any technological response to a crisis is essential not only to its success, but also to ensure that we have a society we are glad to be part of once we return to times of relative calm. Australia would do well to heed this lesson.

Samantha Floreani *works at the intersection of human rights, technology, and feminism. She is currently the Program Lead at Digital Rights Watch where she advocates for human rights in the digital age. She was previously a Privacy and Technology Specialist with Salinger Privacy, a Board Member of the Australian Privacy Foundation, and Program Director for Code Like a Girl.*

Disruptive Technologies, Surveillance as Governance: Data (Un)Democracy in India during COVID-19

PREETI RAGHUNATH

As it raged through the world's largest downgraded democracy, the COVID-19 pandemic not only resulted in a great loss of life in India, but also provided an impetus for authoritarian control. The increase in data collection justified by the pandemic has led to a populist-protectionist form of digital authoritarianism.

In 2017, one of the main architects of India's Aadhaar, the world's largest biometric program, made a presentation on how India must embrace data democracy, recognising the vast potential of using accessible data for profit. Even as the India

Stack – a project to create a unified software platform – had been active for a few years prior, the presentation made it amply clear on what to expect for India's technological development over the following years.

In recent years, India has focused on a deterministic usage of technology with serious implications for human rights, as seen in the use of AI surveillance systems for policing and proposals to govern personal and non-personal data.

Stacking Authoritarianism: Towards an ID Nation

India Stack is a set of tools and pathways for the creation of technology architecture. Led by iSpirt, a host of volunteers and software developers are working on the multi-layered India Stack to build digital "public" goods, catering to the country's digital governance needs. A recent example of this is the Unified Payments Interface (UPI), dubbed as a fintech revolution in India for real-time digital payments. By combining digital payments infrastructure with the Aadhaar biometric system, India Stack is an attempt to exploit what is seen as a booming digital economy. However, those who have been following the India Stack (and iSpirt) story know that the group has withered into defending invasive technologies and the privatisation of what ought to be public technology, along with contributing to trolling and online hate speech against critics. One such anonymous Twitter account harassing Aadhar critics on social media was apparently set up and operated by iSpirt cofounder Sharad Sharma.

The story of India Stack is also a story of the evangelical segment of the transnational Indian technology community's ideology. Technological determinism, embraced by India Stack's proponents, is a unilinear idea of development and progress, which disregards others' ideas, lived experiences and rights. It seeks to institutionalise putting more faith in technology than people. The latest case of caste discrimination by Google against Equality Lab's Thenmozhi Soundararajan is a case in point. A strong belief in a strange mix of protectionism for the Indian technology industry and populist rhetoric and policies seem to guide much of their functioning.

During the pandemic, the CoWIN app was introduced as the sole mechanism to deliver vaccination to India's very large population. But this approach excluded much of India's rural population; according to the Indian Telecom Services Performance Indicator Report, only 34.60 percent of the rural population have internet access, leaving many without the option of informed consent.

In addition, instead of functioning as public infrastructure, activists and ethical technologists accused CoWIN of open-washing (presenting an initiative as open-source despite not meeting all criteria of openness). In this news report, activist Anivar

Aravind suggested that the Open APIs in India's current public digital infrastructure aren't actually open and only promote government access and consolidation of private proprietary interests.

Multiple bugs, privacy concerns, and technology issues aside, the CoWIN app was also used to harvest data to build the database for India's National Digital Health ID program. With GovTech becoming a big part of governance today, India is activating a slew of measures, piggybacking on India Stack to privatise and close off technology architectures from the public. While this is one side of the coin, the other is that such technologies, without adequate safeguards in place, may be used to fuel hate and discrimination, accentuating animosity and spelling catastrophe for India's social fabric. This was seen in how digital platforms have been used to compound anti-Muslim hate during the pandemic. In late March 2020, there was a surge of disinformation targeting Muslim communities following a COVID-19 outbreak linked to the group Tablighi Jamaat. Lists identifying some of the group members and containing their personal details circulated on social media. While it is unclear whether this information came from GovTech platforms, most of the lists circulating online were prepared by authorities and bore officials' signatures. This incident has shown how entire communities can be targeted and caricatured as super-spreaders, with technology being used to promote profiling of individuals.

Surveillance Cultures: Cities of Control

One of the most common manifestations of digital authoritarianism is the deployment of surveillance technology to police, control, and demarcate people. Delhi and Hyderabad's deployment of Facial Recognition Technology (FRT) led Amnesty International to call Hyderabad a 'police state'. Hyderabad, home to some of the biggest multinational technology corporations, has deployed around 600,000 CCTV cameras. This is in addition to the various other apps and technologies at the disposal of Hyderabad's police department to mark, demarcate and surveil.

During the pandemic, AI-based facial recognition systems were deployed to spot violators of pandemic norms set by state and central governments. This process was normalised during the pandemic, and raises serious questions about AI and the right to privacy. Additionally, by tailoring pandemic responses to technological solutionism, the government and its agencies deployed invasive technologies to substitute for governance. This has disastrous implications. For instance, FRT can misinterpret and wrongly identify those tagged as criminals, and can be used to target certain neighbourhoods in the name of predictive and targeted policing, embedding and increasing bias in existing systems.

The pandemic has been used as a pretext for smart and 360-degree policing and surveillance in the name of maintaining COVID-19 protocols. Authorities have piloted the use of FRT systems for "contactless" vaccine delivery, a move that has raised privacy concerns and fears that this would marginalise millions of vulnerable people.

Fluxes and Fissures: Data Governance in India

A third arena that has registered massive fluxes during the pandemic is that of data governance. In a bid to become one of the few countries to govern the area of non-personal data, and to also address personal data protection, the Indian government developed a committee that looked at legalities and governance mechanisms for personal and non-personal data (a demarcation made by the government).

In 2018 the first draft of the Personal Data Protection Bill was released, which set a framework for the governance of personal data. Subsequent versions of the draft bill, however, reflected state intervention in the realm of personal data protection. In the revised 2019 version, the government could access private data by citing national security or public order, exempting its agencies from rules governing the processing of personal data. Even Justice Sri Krishna, who headed the committee that prepared the first draft of the bill, decried these subsequent revisions, saying it could "turn India into an Orwellian state". As of this writing, the government has withdrawn the Data Protection Bill 2019, and has come under criticism for this move.

Concerns over data protection measures have been highlighted during the pandemic, with the government expanding its access to the personal data of millions of people, particularly health data. In an article on technology policy portal MediaNama, lawyer Sarada Mahesh suggested that India's vaccine rollout needed a privacy policy to protect citizen data. Ensuring the security of personal data has become all the more complex with travel opening up and vaccine passports becoming important. However, concerns over the usage of personal data from contact tracing apps remains alive, since it is tied to the digital health ID architecture of India's digital public infrastructure thrust.

Conclusion

India's focus on a deterministic and ideological usage of technology for pandemic management has not only mismanaged the pandemic, but has pushed the country to contend with Orwellian realities. India's tryst with invasive high technology for policing

as governance is eroding digital public infrastructure and consolidating control over people's data and lives.

That the pandemic and subsequent health crisis was used as an opportunity for techno-solutionism, surveillance, and control is worrying and highlights the need to pay much deeper attention to how such crises are weaponised.

Preeti Raghunath *is Lecturer (Communication and Media) at Monash University, Malaysia. Her academic interests lie in communication and media governance, and media anthropology. She is currently working on developing the philosophical and pragmatic approach of Critical Data Governance, and is most interested in using this lens to contextualise and historicise the linkages between people, data, and governance in South and Southeast Asia.*

Vietnam's Zalo Connect: Digital authoritarianism in peer-to-peer aid platforms

TRANG LE

In 2003, Susan Sontag published a book-length essay *Regarding the Pain of Others*, a powerful meditation on the representation of distant sufferings.[1] For Sontag, images of war-torn bodies, smashed houses, and starving children, brought straight to our living rooms via modern media, created a culture of spectatorship that simultaneously allows us to witness and glance away from the trauma of others. She wrote: "Information about what is happening elsewhere, called "news," features conflict and violence […] to which the response is compassion, or indignation, or titillation, or approval, as each misery heaves into view." What Sontag addressed in *Regarding the Pain of Others*

remains timeless, insofar as she reminds us of the power of technology to alter how we come to understand distant sufferings, and how we think those sufferings ought to be addressed.

Twenty years on since Sontag's powerful critique, we are now supplied with countless opportunities not only to witness others' suffering, but also to remotely provide aid and assistance. Since the COVID-19 pandemic, platforms that connect local citizens who are willing to help each other have emerged and thrived in Vietnam amid the lack of a proper welfare regime. Launched during the country's strict August 2021 lockdown, these platforms were lauded as a timely, innovative, and humane technological solution to address the lack of basic necessities—food, medical care, shelter—needed to care for oneself and others.

But while these apps are touted as exemplars of tech for good, they may also engender new vulnerabilities and harms. Platforms to provide aid and protection can also function as a form of digital authoritarianism that limits perceptions of what counts as aid, and what it means to provide it.

Zalo Connect and the intermediation of Vietnam's COVID-19 response

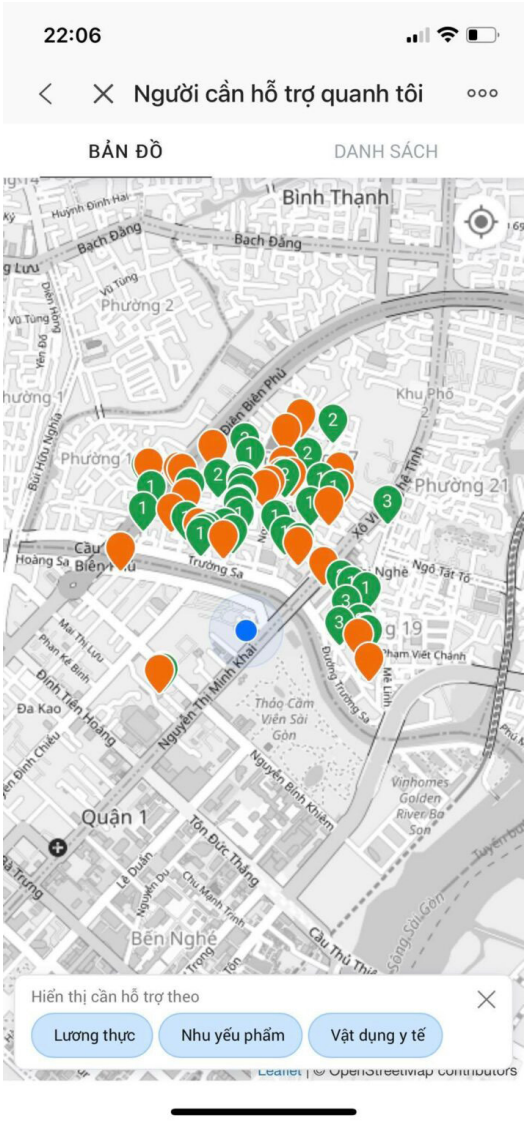
Vietnam had been hailed as a global COVID-19 success story until mid-2021, when the highly contagious Delta variant swept its largest metropolis, Ho Chi Minh City, and other southern provinces. Tough lockdowns were imposed and people were not allowed to leave their homes, even for take-away food. The urban poor in Vietnam have always relied on informal, more affordable food systems such as wet markets and street vendors, but these informal spaces were forced to close as they were deemed unhygienic and potential hotspots for virus contamination. For many precarious daily wage earners who couldn't afford to stockpile food from supermarkets, starvation became a daily reality.

In partnership with the National Centre for Technology, Vietnamese private tech company VNG Corporation developed Zalo Connect, a new feature under the already popular networking platform Zalo that allows users to request emergency help and be matched with a donor willing to provide food, necessities, medical equipment, or medical advice. Zalo Connect's interface also has a map view navigation that enables potential donors to locate nearby people in need. As the health crisis quickly spiraled into a hunger crisis, unsurprisingly 92 percent of the requests for support are reported to be food-related items.[2]

Zalo Connect's interface translates the cityscape and the crisis unfolding within it into a set of orange and green dots, representing people who request emergency assistance. People who have not received any help are represented by orange dots. Once help is

provided, the orange dot will switch to green and information on the number of times they have been assisted will be listed. By clicking on the dots, potential donors can see detailed information regarding vulnerable people's circumstances as well as their specific requests. In only a fortnight since its launch, Zalo Connect reported 85,000 matches.

Zalo Connect exemplifies a humanitarian trend that centres on extracting data from vulnerable communities as a precondition for receiving aid, protection, and justice. How do these platforms perpetuate and legitimise the exploitative logic of data extraction where the beneficiaries are compelled to publish their own miseries in exchange for aid? What are the harms inflicted on these vulnerable communities as images, information, and other data representing their lives and bodies are stored in digital space—but over which they have no control? What is at stake when the pressing task of alleviating suffering during the crisis is framed as an issue of matching supply and demand?



Screenshot of Zalo Connect taken by Phuong Thao, used with permission.

The imperative of self-disclosing miseries: (Self) surveillance and the production of new vulnerabilities and harms

I was overseas when Ho Chi Minh City and its neighbouring provinces entered their strictest lockdown, taking my maternity leave to care for my two-month-old newborn. At the time, my friends in Vietnam occasionally sent me information about people needing emergency help to raise funds for them. Among many requests, I felt the urge to donate to a mother who just gave birth (perhaps because I was in a similar situation then); she was unable to breastfeed her child, yet could not afford baby formula. We sent her a message, and without us requesting any evidence, she immediately sent through all the hospital documents detailing every pregnancy check-up and a certificate showing the date and time of her recent C-section. She must have believed that she and her physical body could not speak with credibility, and that these forms of documentation were seen as more credible conveyors of her circumstances, no matter how intimate, personal, or traumatising they might be.

My encounter with the mother took place via another platform, but in many ways, it exemplifies the kind of social interactions mediated by Zalo Connect—where people in insecure situations are compelled to share information about their sufferings, trauma, and losses, in exchange for aid and protection. Aside from choosing a predefined category of assistance, those seeking aid are prompted to give specific details of their requests. Though not explicitly required by the platform, many people opt to narrate their miseries and hardship, perhaps in a bid to move potential donors. For example, a request reposted on an article about Zalo Connect read: "I need help with food. I'm working at a construction site. My husband passed away and I'm raising two children on my own. One is sick but we can't afford surgery. And now I'm unemployed."[3]

The issue then becomes one of autonomy and control. While the stories are clearly in the control of the persons they are seen to represent, the requesters depend on those stories to bring them aid—thus putting the onus on them to calibrate the kind of story capable of generating sympathy and compelling donors to take action. In other words, the seeming democratisation of access to aid afforded by Zalo Connect reinforces a self-surveilling regime, insofar as the agency and ownership of the story come up against the donor's need for credible evidence and believable narratives.

The self-disclosure of miseries was compounded by contextual factors, such as social distancing measures, that prevented donors from traveling directly to donees' residences and witnessing their plight firsthand.[4] This distant witnessing creates a problem of trust, exacerbated by the pervasive discourse in popular media that seems to draw the line between the "deserving" and "undeserving", "authentic" or "fake" poor. For example, an article from VNexpress featured a donor who was frustrated with many "fake" help messages she encountered, which was taking her ages to "verify" before deciding to help.[5] She did not detail her method of verification, but we might imagine that this entails requesting more proof, more data, more documentation. The border between vigilance and surveillance can be dangerously thin.

Asymmetrical visibility: Reconfiguring relationships between the "helper" and the "helped"

The interface of Zalo Connect allows donors, the relatively privileged group, to look upon the cities as a whole and enclosed space; a place with many suffering bodies, but also as an entire place of kindness. Among many celebratory accounts of Zalo Connect, one succinctly puts it: "Zalo Connect allows for kindness to spread".[6]

The map view of Zalo Connect also allows users to move smoothly from one scale to another so that users can see either the entire crisis-scape or at the minute level of an individual. In other words, potential donors are invited to see the crisis unfolding from the above: an all-seeing, all-knowing God's eye view. We are not the object of surveillance; we are not the victims of many watching eyes.

Viewed in an optimistic light, the relative accessibility of mobile phones, the internet, and social media and their use in facilitating peer-to-peer aid may signal a bottom-up and localised distribution of support. While there is some truth to it, such an interpretation weighs too heavily on the democratic potential of technology. On the surface, there is seemingly no intermediation between donors and donees, just a smooth flow of information and exchange that provides transparency and an emotional bond. However, there is no way for a crisis-affected person to voice for themselves what they demand outside preconceived notions of aid. One media account, for example, described a beneficiary as "demanding"—she allegedly asked for high quality food as her child had a stomach issue—and tagged her request as "fake" simply because she didn't fit the stereotype of "grateful donees" who would readily and enthusiastically accept whatever was given. As Theo Sowa, chief executive of the African Women's Development Fund expressed: "When people portray us as victims, they don't want to ask about solutions. Because people don't ask victims for solutions."[7]

In many ways, the saviour mentality is reproduced beyond the interface of the app; for example, the app is used as a part of a campaign to garner social capital for VNG, earning them more users and partnerships. The media landscape is replete with stories about how these vulnerable groups are grateful for the tool and the assistance they received. The vulnerable communities cannot turn back their gaze. Consequently, while Zalo Connect appears to give voice to otherwise voiceless communities, it is through this asymmetrical visibility and power relations that these communities are dehumanised. The exhibition of orange and green dots representing vulnerable bodies in crisis, oblivious to the diverse demands and needs these communities might have, is regarded only as someone to be seen, not someone (like us) who also sees.

By design, Zalo Connect does not allow for dignified access to aid. There is no framework to limit the amount and nature of the information that should be provided by the beneficiaries. Nor is there any consideration to destroying data about these

vulnerable groups to protect their privacy. In a pandemic, this extra layer of extracting data from vulnerable communities in exchange for aid magnifies the power exercised over such communities, potentially resulting in shame, stigma, and retraumatisation. This also reconfigures new power relations over the most vulnerable communities that have already been more heavily surveilled under ordinary circumstances.

The power of problem framing: how platformising aid abstracts the issue from its systemic context

Zalo Connect illustrates how digital humanitarianism can function as a form of digital authoritarianism, legitimising an extractive relationship that requires a public disclosure of miseries with the very groups they seek to assist.

With each successful matching, the dots representing the beneficiaries switch from orange to green. We, the relatively privileged group, must assume these distressing situations have somehow been resolved. We must assume they have found some respite. But this bittersweet representation should not distract us from asking what harms are not being shown.

Difficult questions, therefore, need to be asked. What problems and solutions are being framed for us? Who benefits from this framing? What does it mean for how we calibrate vulnerability, aid, and protection? Against the context of persistent failure from the state to provide a safety net to its citizens, Zalo Connect's design implies a transactional solution to a structural crisis: The donor sends food, necessities, or medical equipment, and the problem is solved. But the problem of providing the basic goods and services cannot be demoted into a mere problem of matching supply and demand.

Trang Le *is a PhD candidate at Monash's School of Media, Film, and Journalism, and a member of the ARC Centre of Excellence for Automated Decision Making and Society. She researches media technologies, gender, space/place, and datafication. Her work examines why complex social issues are conceived as having technological solutions and what the potential consequences are.*

References

1 Susan Sontag, 'Regarding the Pain of Others', Penguin Books, 2003.

2 Kim Lam, 'Tính năng hỗ trợ người khó khăn do dịch bệnh Zalo Connect mở tại 20 tỉnh thành' [Feature assisting vulnerable people due to the pandemic Zalo Connect launched in 20 cities], last modified 20 August 2021, Thanh Nien https://thanhnien.vn/tinh-nang-ho-tro-nguoi-kho-khan-do-dich-benh-zalo-connect-mo-tai-20-tinh-thanh-post1102796.html

3 Rosie Nguyen, 'Zalo's New Tool Boosts Mutual Aid During Vietnam's Worst Covid Outbreak', last modified 20 August 2021, Vietnamtimes, https://vietnamtimes.org.vn/zalos-new-tool-boosts-mutual-aid-during-vietnams-worst-covid-outbreak-35080.html

4 This is how informal humanitarian assistance in Vietnam had been operating where a citizen would raise funds from their friends and families and travel to the fragile settings to give away their donations. With social distancing measures, all potential donors can see is self-narrated accounts of suffering on help-matching platforms.

5 Luu Quy, 'Tìm người hỗ trợ nhu yếu phẩm qua Zalo [Locating people in need through Zalo], VNExpress, last modified 17 August 2021, https://vnexpress.net/tim-nguoi-ho-tro-nhu-yeu-pham-qua-zalo-4341837.html.

6 Quoc Huy, 'Đánh giá tính năng Zalo Connect: Tính năng mang đậm tình người, dễ dàng kết nối người cho và người nhận nhu yếu phẩm [Evaluating Zalo Connect: a humane feature, easy to connect helpers and the helped]', The Gioi Di Dong, last modified 18 August 2021. https://www.thegioididong.com/tin-tuc/danh-gia-zalo-connect-1375820

7 Jennifer Lentfer, 'Yes, charities want to make an impact. But poverty porn is not the way to do it', last modified 12 Jan 2018, The Guardian, https://www.theguardian.com/voluntary-sector-network/2018/jan/12/charities-stop-poverty-porn-fundraising-ed-sheeran-comic-relief

PeduliLindungi: To Care for and Protect?

SITI ROCHMAH DESYANA

Read this post in Bahasa Indonesia

As the COVID-19 pandemic continues in Indonesia, the government's PeduliLindungi application remains an integral part of daily life. Named by merging the Indonesian words for "care" (*peduli*) and "protect" (*lindungi*), the app claims to do just that, tracking and screening COVID-19 statuses, and providing resources and information on COVID-19. Its existence has become synonymous with and inseparable from the pandemic itself, and people's reliance on the information, access, and resources it offers to protect themselves from COVID-19 comes at the risk of trading off one's rights to data privacy.

As of writing, over 50 million people have downloaded the app from the Google Play Store, making it the top medical app in the country. But as more and more users register and use the app, the severity of concerns regarding the app's security and extensive tracking have also increased.

In September 2021, Indonesian President Joko Widodo's vaccine certificate was leaked online. The incident came just a month after the suspected breach of the Indonesia Electronic Health Alert Card (eHAC) app, which compromised the data of 1.3 million users. The leaks have since triggered public discourse on data security and the amount of personal information collected and stored by PeduliLindungi.

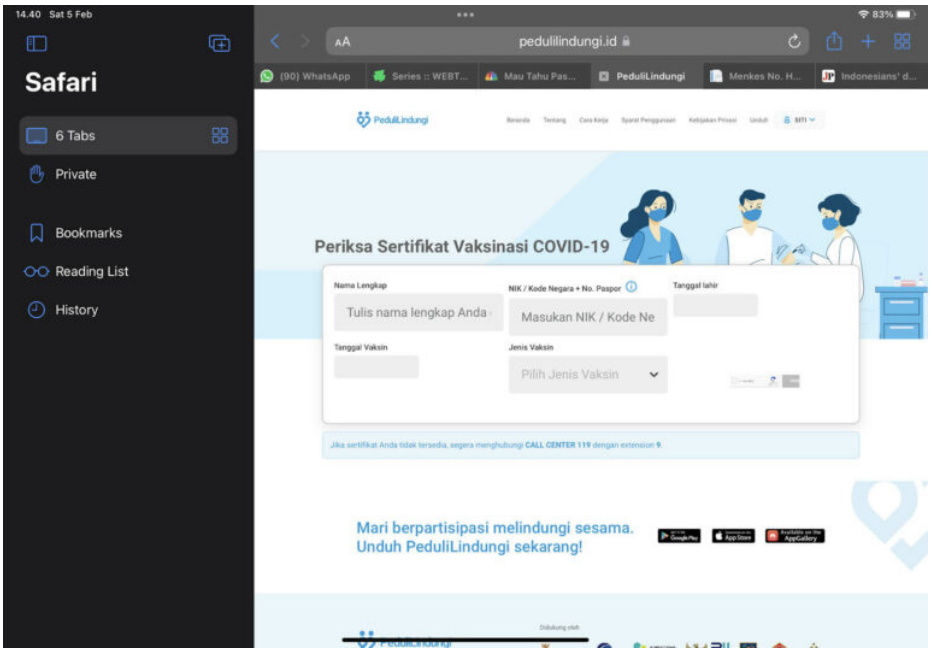
Following the breaches, the Indonesian government has since claimed that the app has secured the data of all users, a response not unlike previous reassurances it has given, after similar breaches in the past. PeduliLindungi thus potentially poses a bigger threat due to its frequency of usage, amount of users, and unique type of information stored, all while leaving Indonesians with little to no legal recourse to protect their data.

A daily ritual: How PeduliLindungi controls average Indonesians' freedom of movement

While the app's usage varies between regions, there is no other government platform that reaches the scale and scope of PeduliLindungi. The main app's interface has also been integrated into 15 other consumer-oriented apps, and there are even plans to turn the app into a digital wallet.

To enter any public place in Indonesia, one must first scan the location's required QR code through PeduliLindungi or any other app interconnected with PeduliLindungi, such as Jakarta's regional app JAKI and the Indonesian startup giant GOJEK. The collected information – such as the user's legal name, ID number, susceptibility to catching COVID-19, current location, and time spent within the facility – are then logged and stored on PeduliLindungi servers. Previous versions of the app had made that information available for users to see under the option "Check-in History". Those who have not formally registered for PeduliLindungi or the other interconnected apps are allowed to enter public space only if they show valid vaccine certificates, which are also hosted by PeduliLindungi and must be accessed through its portals.

When an Indonesian is not formally part of the PeduliLindungi system, there are a number of challenges and hurdles disturbing their daily routines. For example, if one is not able to get a ticket to get vaccinated – whether it is their choice or vaccine unavailability – one will not be allowed to freely use and enter bus stops, train stations, markets, hospitals, office buildings, and other public spaces. The unvaccinated have even reported difficulties in getting treatment from medical facilities, which rely on the PeduliLindungi database to access one's COVID-19 status.



PeduliLindungi users can request for vaccine certificates via the website. As long as you have a full name, ID number, date of birth, and date and type of vaccination, you can access anyone's vaccine certificates. Screenshot taken by the author.

Using the app is now not only necessary, but socially mandatory in order to keep one's freedom of movement. Such measures were argued as justified to curb the spread of COVID-19, despite questions regarding their ability to do so. However, it must be stressed that the government should not only rely on PeduliLindungi to decide who is eligible to access basic needs and public services afforded to the Indonesian public, regardless of people's ability to be vaccinated, get tested for COVID-19, and more.

How secure is the data?

There are also numerous unanswered questions surrounding the digital security of PeduliLindungi. While no classified information stored online can ever be completely secure, the Indonesian government has yet to take adequate action to ensure the security of its various databases.

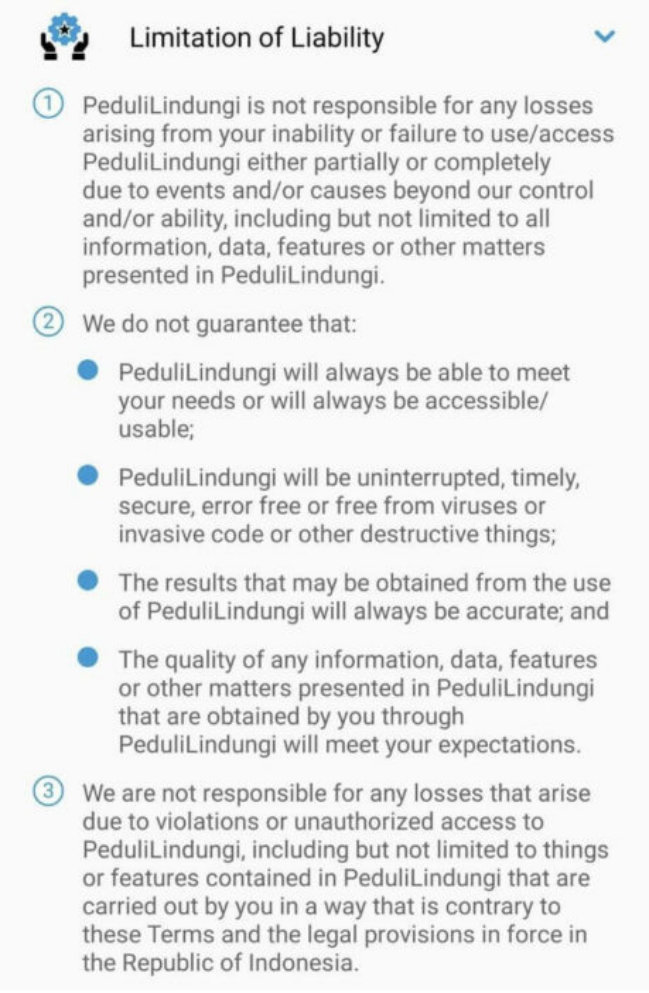
When the eHAC database was leaked in 2021, the government chose to deflect and stress that only the "old, separate eHAC" was compromised. It also did not elaborate on the steps it had taken to secure both versions of eHAC and their interconnected servers (which includes the servers used by PeduliLindungi). In the end, the government simply asked citizens to delete the old eHAC app on their phones.

PeduliLindungi does not escape this lack of accountability. For one, the President's leaked vaccine certificate only showed how easy it was to obtain any certificate – even those not your own. Accessing these on the app requires only a full name, ID number, date of birth, and date and type of vaccination – information that can easily be found on social media or even through carelessly discarded paper documents.

In the President's case, investigators found that his information was obtained through PCare, a separate application by the Ministry of Health and which is used by healthcare providers to upload a user's vaccination data to PeduliLindungi servers. The connection between both applications remains unclear.

The issue only compounds with the interconnectivity of PeduliLindungi with other third-party applications. For example, the app is connected to Google and other third-party software providers that track users' locations when entering and exiting public spaces, and when using public transportation. A previous version of the PeduliLindungi mobile app allegedly contained anomalies, including manual data storage within the application and sending said data to an external, non-Indonesian website. The app had also in the past sent users' names and kinds of devices to a subsidiary of PT Telkom, Indonesia's state-run telecommunication company with servers in Singapore.

But despite evidence that third-party applications may have led to data breaches on other government apps, PeduliLindungi's latest privacy policy maintains a no-liability clause for "violations or unauthorized access", which include how third parties use PeduliLindungi's data. The app also claims no liability for damaging results emerging from its system's failure and disturbances.



PeduliLindungi's Limitation of Liability on the mobile version of the app. Screenshot taken by the author.

Lack of protection, regulation, and accountability continues on

Despite large numbers of infections, the public continues to debate whether the monitoring and tracking done by PeduliLindungi are necessary to curb the spread of COVID-19. Regardless of which side of the debate you are on, the Indonesian government's responses to past data breaches and other concerning events fail to address the root of the problem: the security of the PeduliLindungi servers and the data privacy of its users.

The government never published the results of PeduliLindungi's initial security audit, which would have informed the public of the safety and security of the app before its implementation. There have been no updates of an additional audit performed after the supposed leak of the President's certificate.

PeduliLindungi is also still not registered under the government's own Electronic System Organizers – a requirement for public servers as per regulation.

The Indonesia Internet Governance Forum (ID-IGF)'s advice regarding improvements that may be made to guarantee the safety and privacy of the app has also been largely unheeded, despite the fact that it was directly communicated towards one of the app's stakeholders on national television.

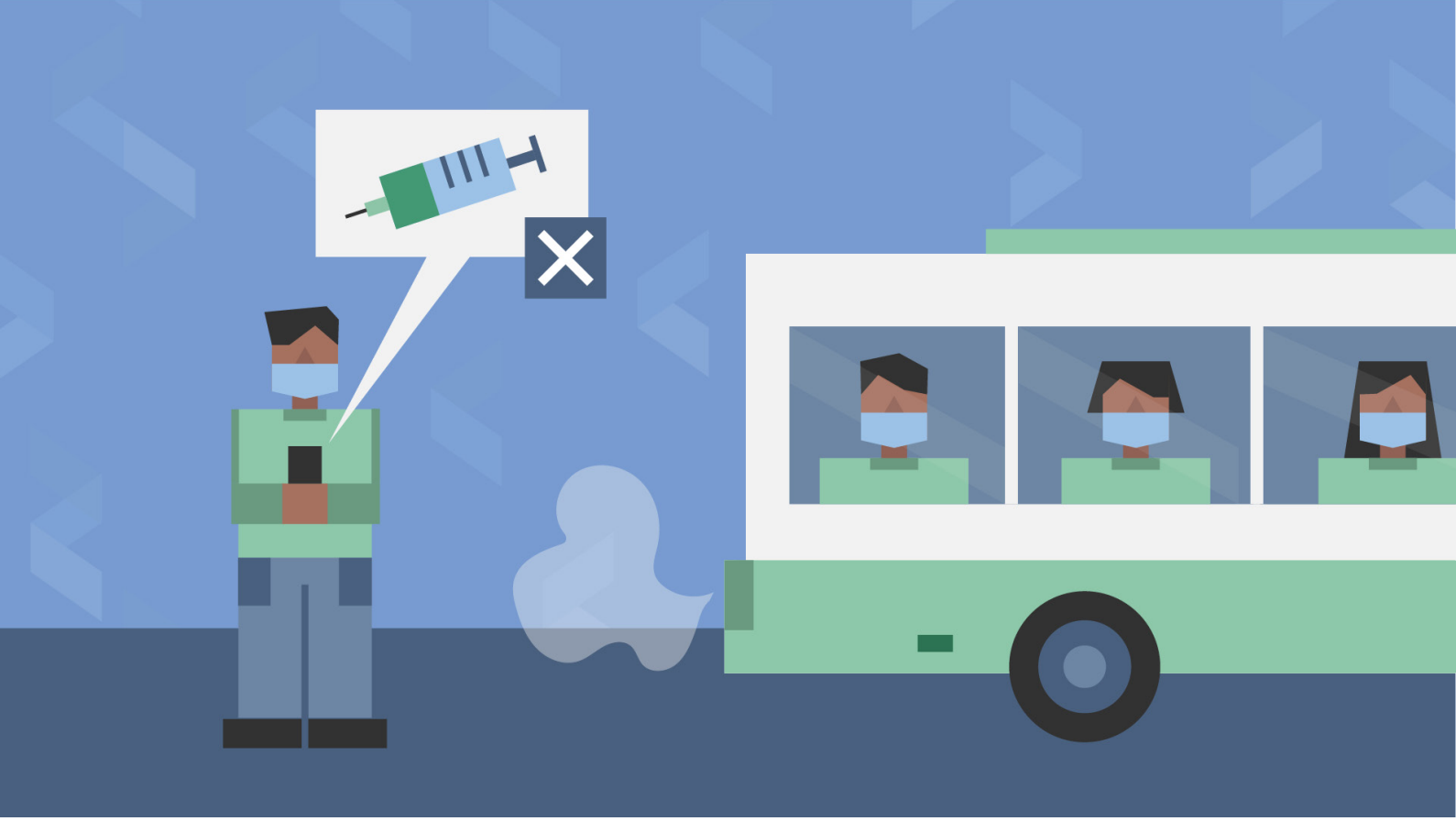
The citizens are once again bearing the brunt of this lack of protection, regulation, and accountability. Indonesians sacrificed their freedom of movement and privacy, and entrusted their data to the government, under the premise that doing so will prevent the further spread of the virus and pave the way towards the end of the pandemic.

Worse, Indonesia currently has no specified legislation concerning the protection of data privacy. While there are provisions regulating consent to individual data usage, they are scattered around various levels of law.

The Legislation Concerning Electronic Information and Transaction, for example, regulated the consent that must be acquired from users for the usage of personal data obtained from electronic media. It further stated that should a court rule that the data used has been deemed improper and is causing damage, then the electronic media hosting the data shall promptly delete the information. There are no discussions concerning the consequences of the electronic media for improper utilisation of personal data, nor is there specific regulation on reparations for the damages induced by the improper usage. The currently existing Ministry Regulation concerning Protection of Private Data under Electronic System exists more like a guideline that contains no punitive or consequential clauses for those who breach the rule's terms. While there is a draft for Personal Data Protection Laws, it is still stuck for deliberation under the House of Representatives, and few improvements have been made so far.

As PeduliLindungi and the government continue to fumble in its operations, and as these concerns are brushed under the rug, one needs to ask: *Is PeduliLindungi really caring for and protecting the Indonesian public?*

Siti Rochmah Desyana *is an observer of human rights issues, and is especially interested in the matters of equality and justice. She currently works in International NGO Forum on Indonesian Development (INFID) for the In-Equality Program, and writes about the world in her free time.*



Risking health for mobility? Limitations of Indonesia's pandemic management tool

GUEST WRITER

Read this post in Bahasa Indonesia

Since the COVID-19 vaccine rollout began in January 2021, people in Indonesia have been clamouring to get vaccinated. Widespread media coverage on rising cases, government campaigns touting the efficacy of vaccines to increase immunity, and fear of getting sick drove many to queue at their local health centres. As of April 2022, 59 percent of its 270 million population have been vaccinated.

Immunocompromised people like me had concerns about the safety of vaccines due to our medical conditions, and so many of us opted to wait and take extra precautions (such as avoiding crowds) to ensure our safety. In July 2021, the Indonesian government launched the PeduliLindungi application, intended as a pandemic management tool for implementing health protocols, contact tracing, and monitoring vaccination status. Since its launch, PeduliLindungi – and one's vaccination status as reflected on the app – has become mandatory for free movement in public spaces. People have to install the app on their smartphones to be able to scan QR codes at facilities such as banks, shops, and health centres before being allowed entry.

This requirement to be part of the PeduliLindungi system and show my vaccination status to access basic services created major hurdles in my daily routines. My freedom of movement became restricted, as the government relied on apps like PeduliLindungi to control the pandemic – this, despite concerns over data privacy and whether or not such digital tools are an effective pandemic management tool in the first place. (*Learn more about PeduliLindungi in another article from the Pandemic of Control series*.)

Restrictions to free movement

Initially, I did not want to get vaccinated because of my immunocompromised status. Ten years ago, I was diagnosed with rheumatoid arthritis, an autoimmune disease in which my immune system attacks healthy cells in my body by mistake and causes inflammation. Because of my condition, I have been selective in taking medication, including vaccines.

Problems began to arise when various institutions started to require proof of vaccination as a condition to enter public spaces such as offices, banks, and malls. In early 2022, Luhut Binsar Panjaitan, Indonesian Coordinating Minister for Maritime Affairs and Investment, made a statement that only people who were vaccinated twice could enter public facilities. This would be reflected in the PeduliLindungi app, which shows people's health status through four colour categories:

- Black: User is positive for COVID-19 or has a history of close contact with COVID-19 patients
- Red: User is not vaccinated or has been exposed to a COVID-19 case; not allowed to enter public areas
- Yellow: User has received a first dose of the vaccine; allowed to enter public places after further verification and in compliance with strict health protocols
- Green: User is fully vaccinated and allowed to enter public places

Because I was not vaccinated, I had difficulties moving around as my job required travelling out of town. To use public transportation, I needed a doctor's note for each

trip. I could also secure a certificate about my autoimmune disease from an internal medicine doctor, but it would require me to take several tests and go to a hospital more than 20 kilometres away from my house in Yogyakarta. Additionally, unvaccinated people like me were required to take RT-PCR tests, which could only be done at major laboratories and hospitals (quite a distance from my home), with results released in a couple of days.

An ineffective pandemic management tool?

Governments around the world have resorted to apps like PeduliLindungi to restrict freedom of movement for the unvaccinated as part of their COVID-19 mitigation response. Proponents argue that mandating the use of such tools drives up vaccination rates (this, despite legitimate concerns from immunocompromised people like me). But sceptics point out that not only do these tools present a host of scientific, ethical, and legal issues that may only exacerbate inequalities, the use of these digital platforms also poses risks to privacy and digital security. The primary purpose of the passports was to mitigate infection; unfortunately it has long been clear that the vaccine and the passports are ineffective in this regard.

PeduliLindungi, for instance, has a massive database – over 50 million people have already downloaded the app. But questions remain on whether the information kept by the system is secure. There are also concerns over the app's interconnectivity with other third-party applications and possible data breaches that may arise from it, as well as PeduliLindungi's no-liability clause for "violations or unauthorised access".

These issues call into question whether using apps like PeduliLindungi – with its data security issues and potential to reinforce discriminatory practices by restricting free movement – is the appropriate response to the primary purpose of reducing COVID-19 transmission.

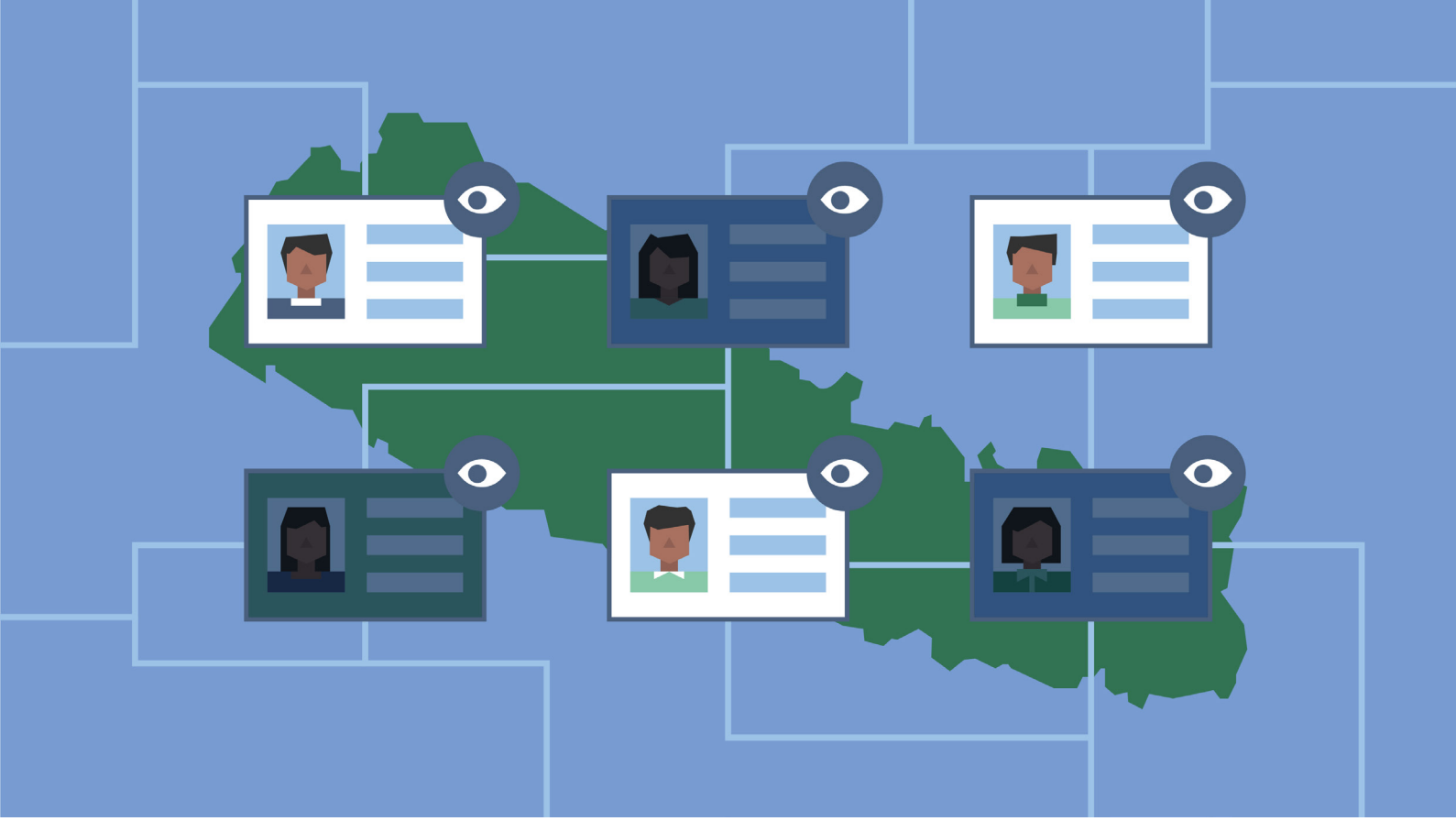
Need for due diligence and scrutiny

I had to wait until there was a safer vaccine, but I finally chose to be vaccinated because of these troubles on travelling and going about with daily activities. Ideally, I should have gone to a doctor and undergone a series of tests before getting vaccinated. But because my house was far away from the city, I did not do that.

There were others like me who took such risks. But for many people, the cost of going to a doctor can be prohibitive. In Yogyakarta, for instance, the minimum wage per month is less than 2,000,000 rupiah (approximately 138 USD), and tests to determine if an immunocompromised person can safely take the vaccine can cost 1,000,000 rupiah (around 69 USD).

Amid legitimate concerns over the health impact of vaccines in immunocompromised people, people like me have chosen to take the vaccine and have the PeduliLindungi app allow us more freedom of movement in our daily routines. While certain concessions may be made to safeguard public health, mandating the use of tools like PeduliLindungi should be closely studied instead of hastily implemented, to ensure that authorities adopt solutions that work effectively to curb transmission while protecting against using digital tools that facilitate social exclusion and the curtailment of digital and human rights.

The writer's identity has been withheld at their request.



Towards digital authoritarianism in Nepal: Surveillance, data collection, and online repression

SAMIK KHAREL

In Nepal, the COVID-19 pandemic sped up the process of bringing public and private services online: from food delivery and shopping to government transactions. These changes came with many downsides, with data and privacy rights often not respected.

Nepal does not yet have the technology and expertise to be globally competitive in the digital world. Instead, it has looked to its closest neighbours, China and India, for guidance. However, seeking ideas from countries that have largely failed to respect basic digital rights puts Nepal in a vulnerable position.

From questionable data collection practices to the curtailment of free speech, Nepal is leaning towards an authoritarian model of internet control, with COVID-19 accelerating this development.

Influence from China and India

China holds a poor digital rights record, with rights groups flagging its online censorship rules and deployment of mass surveillance against the Uyghur Muslims, among other rights violations. Similarly, India has been widely criticised for procuring spyware, imposing internet shutdowns, and passing IT laws that do not conform to global rights norms.

In 2019, Nepali media reported on government plans to mount over 21,000 CCTV cameras for street level surveillance. This is in addition to the thousands of surveillance cameras that are already installed in the Kathmandu Valley. Authorities say the cameras deter criminal activity, but they have also been used by police to monitor protests and other forms of expression. During the COVID-19 pandemic, police used these cameras as well as drones to monitor people's movements and adherence to lockdown rules, publicly flaunting their use of this technology on their official YouTube channel.

In April 2022, a major Nepali daily reported that the government had purchased the Pegasus spyware system and handed it to the Nepal Army for trial use. While the government claims the system is to ensure citizen safety and security, there has been widespread criticism of the spyware and its misuse by governments around the world.

As these surveillance practices become entrenched in Nepal, there is a growing risk that these technologies will be used to curtail people's digital rights, especially as COVID-19 has pushed so much of daily life in digital spaces.

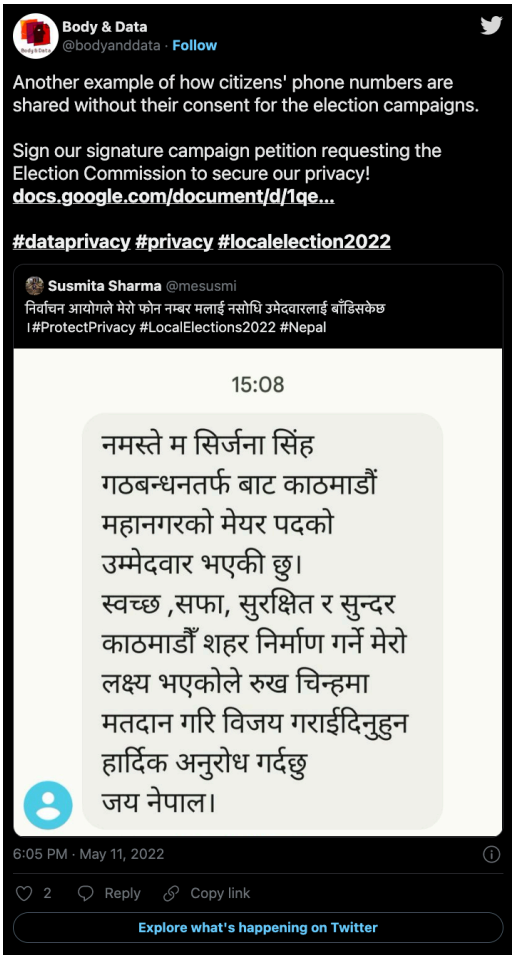
Massive data collection, lack of data security

The government approach to COVID-19 vaccination built in a huge amount of personal data collection. To date, 70 percent of the total population has been vaccinated, requiring more than 20 million people to share their personal information with the government, including to obtain an official vaccine certificate. However, there are questions on whether this massive dataset of personal information is kept secure.

When the government announced booster shots for frontline workers in mid-January 2022, journalist Rajendra Rai (name changed) rushed to the vaccination centre. While waiting his turn, he filled out a vaccination form on the health ministry website via his phone. The form required personal information including his name, birthdate, and address, but also had questions on ethnicity and occupation. After registering online, Rajendra received a confirmation number with a QR code.

If critically reviewed, the personal information in these forms could be used as a weapon by political parties and the state, especially with the federal and provincial elections coming up in late 2022.

Who ensures the safety of the collected citizen data? There have been previous instances of potential data misuse that put into question the government's ability to ensure data security. In the 2022 local elections, voters from particular areas received SMSs and emails from political parties; it is unclear how they obtained voters' contact details and there are suspicions that these were sourced from public service forms submitted to the government.



Body and Data, a digital rights organisation in Nepal, flagged privacy issues related to election campaigns

The Election Commission of Nepal also came under fire for publicly releasing a list of the 17.7 million voters on its website, which included details of the voters' names, age, gender, voting booth, voter ID number, and even their parents' and spouses' names. While civil society and rights groups criticised this privacy breach, authorities did not remove the list, arguing that "there should be no concern of a breach of

privacy" because the data did not include voters' photos, thumbprints, and phone numbers.

The government's response suggests authorities do not sufficiently understand the risks associated with a lack of digital security safeguards. Officials appointed to oversee the vaccine registration process are often unaware of where the data is being stored, how long it will be stored, and how it will be used, according to an anonymous, personal source from the health ministry. How, then, can one be assured that their personal data is secure?

Although civil society, human rights defenders, and concerned individuals have nudged the government to be more responsible with data, Nepal has yet to enact comprehensive data protection and privacy laws. Citizens also lack sufficient awareness and understanding of the potential for data misuse.

Restrictions on free speech

In 2020, Nepal was ranked 112th out of 180 countries in Reporters Without Borders' Press Freedom Index. The pandemic provided the government with an opportunity to undermine press freedom further, in an attempt to control public narratives on the health situation. Nepalese journalists were attacked, censored, and arrested over their critical reporting of the government's COVID-19 response. Police detained Lok Karki, a reporter for Radio Dhangadhi, for filming a disagreement over the distribution of food and relief goods. Nagarik News bureau chief Nagendra Upadhyay received threatening messages from a regional government official over his report that the official's wife had been driven in a government car at the height of the lockdown. In March 2020, a report on online news portal Kathmandu Press was taken down following pressure from the prime minister's aide. This report alleged relatives of several high-ranking government officials were involved in the purchase of expensive medical equipment from China.

In April 2020, journalists reported about an exodus of workers from the Kathmandu Valley as a result of COVID-19 lockdowns. Reacting to the news, the prime minister told the editors of government newspapers that he found the reports "mysterious" – questioning their very basis. These comments were followed by a government-orchestrated online harassment campaign against journalist Binu Subedi using bogus Twitter accounts.

During this time, the government has continued to use the 2006 Electronic Transaction Act (ETA) to arbitrarily detain those criticising the government and leaders of the ruling party. The ETA, initially drafted to regulate financial scams, has become a convenient tool to criminalise speech online. Section 47 of the Act prohibits the electronic publication or display of material deemed illegal under existing laws, but is so broad to include those "which may be contrary to the public morality or decent behaviour" or materials which may spread hate, jealousy or

jeopardise "harmonious relations" among the people. This law was used against Radio Nepal board member Deepak Pathak, who was arrested in April 2020 for defaming Nepal Communist Party leader Pushpa Kamal Dahal on social media.

There is a proposed law seeking to replace the ETA: the Information Technology (IT) Bill, which would give the state the power to censor online content it deems offensive. The bill also includes provisions for arrests and jail terms for anyone posting content deemed to be against "national unity, self-respect, national interest, relationship between federal units". Similar to criticism of the ETA, however, this proposed law contains provisions that are vague and open to interpretation and possible misuse.

Worse than the IT Bill is the proposed Social Media Directive 2021, which would compel social media companies to register in Nepal and abide by the country's laws. The proposed directive has been widely criticised for its intent to regulate content on social media, opening the door for further state censorship. By laying out only a vague idea of what constitutes illegal content, all those who criticise power structures, or use humour and sarcasm against the state, may face punishment. The directive also targets anonymity, threatening people's free expression. The main purpose of the directive is to control online discourse, minimise public engagement in controversial state affairs, and neutralise voices critical of the government.

The government's pandemic response has opened the door to a wide range of threats to human and digital rights in Nepal – from the crackdown on critical voices to the lack of safeguards for digital data, and laws curtailing free speech. With the influence of its neighbours with poor digital rights records, Nepal must decide on its own path if it envisions a free, egalitarian, and democratic digital ecosystem.

Samik Kharel *is a freelance journalist who has previously reported for various national and international media, including Al Jazeera, Deutsche Presse-Agentur (DPA), The Canberra Times, The Kathmandu Post, and The Record Nepal, among others. He also writes and researches on technology, ethics, access and internet culture, and AI.*

In Sri Lanka, state-sponsored disinformation and suppression of dissent taint COVID-19 response

HARINDRINI COREA

In the midst of the COVID-19 pandemic, the United Nations Office of the High Commissioner for Human Rights released a report on Sri Lanka's "alarming path towards the recurrence of grave human rights violations". The country, even before the onset of the pandemic, saw the following trends:

- Militarisation of civilian government functions;
- Reversal of Constitutional safeguards;
- Political obstruction of accountability for crimes and human rights violations;

- Majoritarian and exclusionary rhetoric;
- Surveillance and obstruction of civil society; and,
- Shrinking democratic space.

These trends continue today, further fuelled by a 2020 Constitutional amendment expanding the powers of Sri Lankan President Gotabaya Rajapaksa. In practice, the power to enact COVID-19 mandates was concentrated with the President, with limited checks and balances from other democratic institutions.

This concentration of power, coupled with the government's highly militarised response to the COVID-19 pandemic and state-sponsored disinformation tactics, reinforced the President's authoritarian agenda and a climate of fear and censorship that continues amid the 2022 national protests due to the current economic crisis.

In this context, this article will explore the use of the digital space as a tool by the government to further an authoritarian agenda. The article also highlights the impact of all this on the rights and freedoms of citizens of Sri Lanka.

State-sponsored disinformation against the Muslim community

The government pandemic response has been criticised for its problematic measures, which include the criminalisation and marginalisation of COVID-19 patients, and alleged police abuses against citizens who question and refuse to comply. Critics who protested against the illegal, ad-hoc, and discriminatory nature of the pandemic response were simultaneously silenced through arrests, surveillance, harassment, and intimidation.

Such measures have disproportionately affected Muslims, a minority community in a country where the majority of the population is Singhalese. Pervasive narratives against the minority Muslim community have historically led to online hate speech and physical violence (documented in 2014, 2018, and 2019). These Islamophobic narratives further intensified during the pandemic, with Sri Lankan officials "stoking communal hate" and government policies discriminatory against Muslims.

Even more problematic, such measures were supported through proxies of the state, including private media entities. One notable instance was in April 2020, when the government's chief epidemiologist promoted a false narrative that burials of COVID-19 patients – a common religious practice by Muslims – could contaminate groundwater and spread the virus. The government then mandated the cremation for all victims of COVID-19. These measures directly violated Islamic burial practices, and even the best practices stipulated by the World Health Organization which permitted either burials or cremations for those who died from COVID-19. And yet, private media, such as Derana

and HiruTV amplified the statements of individuals who were spreading misinformation around the possible impact of the burial of COVID-infected bodies.

A highly militarised COVID-19 reposnse

At present, the Telecommunications Regulatory Commission of Sri Lanka (TRCSL) lacks the independence it needs to protect citizens from unwarranted surveillance. In December 2019, retired Defence Secretary Major General Kamal Gunaratne was appointed chairman of the TRCSL; in November 2020, the TRCSL and several other bodies were brought under the Technology Ministry—all directly under the purview of the President.

Internet service providers (ISPs), such as Dialog and SLT Mobitel, do not appear to disclose data about government demands for user information or notify their users if their data has been accessed by the government. Nevertheless, in 2013, Dialog's CEO stated that telecommunications companies "have to be compliant with requests from the government". Furthermore, there are no legal provisions that require ISPs to even disclose such information in the first place.

The appointment of military personnel to key positions in the government normalised military involvement and tactics in civilian affairs, framing the pandemic as a security threat rather than as a public health crisis.

General Shavendra Silva, commander of the Sri Lanka Army, was appointed by the President (also a former defence secretary) to head the National Operation Centre for the Prevention of COVID-19 Outbreak. Military personnel was also appointed to coordinate the pandemic response across the country. For instance, military intelligence officers obtained the cell phone numbers of COVID-19 patients from service providers to track down those who had close contact with such patients or those who "evaded" quarantine. This was despite the prohibition of extrajudicial surveillance of personal communications under the Telecommunications Act No. 27 of 1996.

In addition to this use of surveillance, there are also claims of intelligence officers using Pegasus software. Opposition Member of Parliament Harin Fernando made remarks that the government had begun using Pegasus spyware in March 2021. An anonymous Twitter user also claimed that the Defence Ministry had activated the Pegasus spyware suite with the cooperation of Dialog Axiata and Mobitel with specific targets of "lawyers, activists, journalists, judges, some retired cops, and even senior Cabinet members seen as disloyal to the President". Dialog has since said the allegations were false. Nevertheless, representatives of the government have stated that the Intelligence Unit has not made a request for the software to be purchased, but that the government would consider it if such a request is made.

Crackdown on dissent

On top of this surveillance, individuals who have criticised either the President or the government's COVID-19 response have been arrested throughout 2020 and 2021.

As part of the repressive crackdown on online dissent, there was an attempt to bring in laws to counter disinformation. However, the weaponisation of existing laws, such as the International Covenant on Civil and Political Rights Act No. 56 of 2007 and the Computer Crimes Act No.24 of 2007, against social media users peacefully exercising their right to freedom of expression raises concerns over the introduction of any legal framework that could provide wide discretionary powers to the executive to suppress free speech.

In 2020, the Police Media Division issued a letter to the Criminal Investigations Department and the officers in charge of police stations across the country to arrest not only persons who made or shared "false or malicious" content on social media, but even those who criticised government officials involved in preventing the spread of the pandemic. The government later clarified that the police internal directive only applied to cases in which the "fake or malicious" information contravened laws surrounding the duties of public officers and not mere criticism of the government.

A notable illegal and arbitrary arrest of an individual under both the ICCPR Act and the Computer Crimes Act was that of Ramzy Razeek, a retired government official who often uses social media to comment on social and political affairs. In an April 2020 post, he called for an "ideological jihad (struggle)", using the pen and keyboard as weapons, against the mandatory cremation policy. Ramzy Razeek was detained without charges or proper access to a lawyer and medical care for five months until being released on bail in September 2020. He continues to face the threat of arrest and formal charges against him to this date.

In June 2021, police headquarters issued a statement emphasising that persons who published false news on social media might be arrested without warrants. Five months later, Additional Secretary Dhammika Muthugala, on behalf of the Secretary of Home Affairs State Ministry, issued a letter warning public servants against criticising the government and its policies on social media. The letter stated that the Ministry would take disciplinary action against those who bring the Public Service into disrepute by posting social media comments critical of the government and its policies.

In January 2022, the Senior Superintendent of Police was quoted by a local newspaper as stating that the sharing or posting of content that is detrimental to the image of the President on social media platforms has been prohibited. No such law prohibits this. However, the policy was enforced in the arrest of a woman who merely shared a post about the President being hooted at while travelling.

Protesting authoritarian measures post-pandemic lockdowns

Government initiatives for contact tracing and quarantine compliance as part of the pandemic response have also fed into broader attempts by the government to establish digital databases with details of citizens. Concerns over these attempts have since been raised.

The government's pandemic strategy laid the foundation for the President's increasingly authoritarian response to the exercise of citizens' constitutional rights both in the physical realm and on the internet. But the unprecedented people's revolution in the midst of an economic crisis post-pandemic lockdowns appears to reject state disinformation and narratives, defy surveillance, and resist intimidation and threats of arrests in the pursuit of finally ending President Rajapaksa's authoritarian reign. While the government has used short-lived curfews, a state of emergency, and a 15-hour social media ban to stop the protests and suppress dissent, the protests are growing only stronger by the day.

Harindrini Corea *is an Attorney at Law who holds a Bachelor of Laws (Hons) from the University of London and also a Diploma in Forensic Medicine and Science from the University of Colombo. Currently a Legal Officer at Hashtag Generation, her research interests are in fundamental rights, the criminal justice system, digital rights and social justice.*

How the economically marginalised navigate digital adoption in India amid the pandemic

VAISHNAVI AND ANISH MISHRA

The COVID-19 pandemic sped up the adoption of digital technologies by five years. However, the pivot towards digitisation is excluding those with little to no access to digital services. As part of its pandemic response, India implemented one of the strictest lockdowns in the world, forcing citizens to access most basic services digitally – banking, telemedicine, and social services, among others. While a small percentage of the population was ready to jump into the digital world, the majority had no choice but to scramble to access these digital resources in the first place, leaving them vulnerable to exploitation.

In India, 84 percent of the population has access to mobile phones, but only 43 percent have internet access. This disparity in mobile phone and internet access also exists in terms of age, location, gender, caste and language, among other factors. Indian women are 15 percent less likely to own a mobile phone, and 33 percent less likely to use mobile internet services than men.

The digital divide affects the most vulnerable in rural areas. According to the 75th round of the National Sample Survey, only 13 percent of people over five years of age in rural areas have the ability to use the internet, compared to 37 percent in urban areas. The COVID-19 lockdowns highlighted this digital divide further: between March 2020 to February 2021, Indian schools were fully closed for 62 percent of instruction days and partially for 38 percent. Only 15 percent of children from rural areas had access to education. Aside from education, this disparity in access to digital services persists in other areas of daily life, such as telemedicine, banking, and e-governance.

Digital inequity is based not only on quantitative metrics (such as the number of smartphone users in India) but also on qualitative indications of what one aims to do with such devices and the clear discrepancy between these intended uses and one's actual access to technology.

Perspectives from the ground

In March 2020, when the Indian government announced an unplanned nationwide lockdown with a four-hour notice, 90 percent of the country's workforce – informal workers – faced a huge crisis. Around 80 percent of the workers were stranded in various parts of the country with less than Rs.100 (less than 2 USD). We spoke to fellows of the Stranded Workers Action Network (SWAN), a group advocating for migrant workers' issues, to understand how they felt about the push for digital adoption in accessing basic social services.

Seema, 27, is a trained nursing support staff from Simdega, Jharkhand, and also a SWAN fellow. She believes digital adoption can be beneficial, citing how she has been able to assist a few people from her community register online for their e-shram cards (a social security scheme for unorganised sector workers). However, she immediately added that knowing how to use these online registration portals is limited to a select few. In theory, one can register for various government schemes and certificates (such as a Caste Certificate, or a proof of identity) by themselves. In reality, however, the use of online systems has led to the creation of a whole set of middlemen, including private vendors with a computer and internet connection, offering to undertake the registration process for a certain fee. Seema talks of how this setup monopolises information into the hands of a few. To register for a certificate, for instance, one needs to supply an identification document and proof of address, among other requirements.

Once this information is uploaded by the workers onto the portal through these private vendors, the workers face an uncertain wait for a document that may or may not reach them. They have no mechanism to track the progress of their applications, forcing them to rely on private vendors.

One wonders: Was it not the same case even before digitisation? While not ideal, Seema says non-digitised processes offered them options. "At least before, we could plead with the district officer, visit him every day and follow up with him to get them to issue the certificate even if it means to plead with them. We were able to use our social connections. Now, we are helpless", she said.

Seema added: "We don't know what is going on online, nor do we know how to follow up on an application, and are left at the mercy of the operators to tell us what's happening".

Gulzar, another worker from Jharkhand who was stranded in Goa during the lockdown, echoes the same concerns. While implementation of technology can be helpful to many people, he feels that for villagers, it isn't of much use so far. Gulzar says they get hoodwinked into sharing personal information, such as banking details, resulting in multiple people losing money from their accounts. They are not equipped to do mobile banking by themselves, so if they want to check if their wages are deposited in their accounts, they often have to rely on either officials or middlemen to check their account balance or the status of their wages.

The main problem that emerges from the narratives of Seema and Gulzar is not that of corruption or delays – for it can certainly be argued that this can happen in any system. The glaring issue is that the common person has been completely left out in a digital society, excluding them from exercising their basic rights and entitlements. To solve systemic inequities, technocratic solutions like digital adoption have been touted as the end solution for all societal and systemic problems – including the problems posed by COVID-19 mobility restrictions. However, as Seema explains, this shift to digital systems has been forced upon them and they never had a choice to begin with.

They are thus left with a system they do not know how to use, allowing them to be exploited, and a system they do not understand leaves them unable to hold anyone accountable. Gulzar's concern about the middlemen points directly to the ambiguity in accountability that online systems bring and the lack of any support and training in supporting the marginalised in adapting to digital technology. Thus, digital adoption is furthering existing inequities and creating new power structures that put the vulnerable in a disadvantageous position.

The stone's throw from digitisation to digital surveillance

Is there then a link between this rapid digitisation of services, its inaccessibility, and it becoming digital surveillance? The collection, use, and control of personal information become evident in the narratives we present here. We believe it is, and this argument stems from what Seema told us at the end of our conversation. We asked her: do people have any concerns about where their data goes? Does the digitisation of services translate into concern about digital rights and privacy? She says they are worried about the consequences of uploading data online, for fear that it can be used for purposes other than that for which it is solicited. Interestingly, the misuse Seema refers to is governmental misuse and not concerns of third party access to her data. It is a concern that the data they surrender online will be used to prosecute them if ever needed.

When asked the same question, Gulzar tells us: "It's not just a concern, I have seen people [end] up in trouble because of sharing these details online!" A friend of his had to share banking details for an online registration, and soon bizarrely had a First Information Report (document prepared by the police related to the commission of an offence) against his name with charges of hacking linked back to his account. "My friend is illiterate. How can he even be capable of hacking, something that requires using a computer?" says Gulzar. He cites another example on the risks of sharing personal information with middlemen, such as bank account details. At times, these middlemen would simply say that the bank accounts are empty despite the workers having been paid, blaming some online issues while pocketing the money. "We simply don't know what to do when faced with trouble. At least before I could write an application or something, but now I don't even know what the problem is", he said.

The compulsion of having to rely on a digital system, coupled with it being a system that leaves them vulnerable to exploitation, shows how their lives are now shaped (unwillingly) through technology. The government has also been actively enforcing this inclusion into digital systems, going beyond social security schemes and encompassing other aspects. In June 2021, 22,000 Accredited Social Health Activist (ASHA) workers (the primary health workers of India) in Haryana protested against a mobile app that was made compulsory by the National Health Mission of India. Health workers were mandated to download a Mobile Device Management (MDM) application to report and track their work, violating their digital privacy. The application, "MDM 360 shield", was forcefully installed on the workers' personal phones by local health department officials. In cases where they were provided with a new phone, the workers were not informed that the application had been pre-installed on the devices.

This development poses serious concerns, as India is yet to have comprehensive data protection policies despite having a large biometric database. There is no actual legal framework on data quality and proportionality, data transparency, or mandating

a Data Protection Authority to properly address and cover data protection issues in accordance with the principles of the European Union's Data Protection Directive, OECD Guidelines on the Protection of Privacy, or International Safe Harbor Privacy Principles. The latest draft of India's Personal Data Protection bill in 2019, tabled in the parliament in December 2021, exempts the government from its purview. The bill prioritises economic interests over the need to protect personal information privacy and has received criticism from digital rights activists.

The push for digitisation during the pandemic – whether for health management or to keep daily activities going amid lockdowns – has deepened the digital divide. Escalated digital adoption without adequate policy protections can exclude the already marginalised even more, yet no one can be held accountable because India lacks any comprehensive framework to do so. While access to social benefits and privacy are recognised as fundamental rights, any program or policy that isn't inclusive is bound to encourage a development paradigm that leaves the vulnerable behind. The narratives of Seema and Gulzar and the experience of the ASHA workers all point to this effect.

Vaishnavi *is currently the policy expert in Greater Chennai Corporation's Gender and Policy lab. She is a social sector researcher with interests in local democracy, political participation, and gender. She can be reached at vaishnavi.cnathan@gmail.com.*

Anish *is currently an MPhil student in the Hong Kong University of Science and Technology. He does environmental philosophy with a focus on Aesthetics, Buddhism, and Social Justice. He can be reached at amishraac@connect.ust.hk.*

Anish and Vaishnavi are part of the Stranded Workers Action Network (SWAN), a voluntary network working with informal workers through relief and fellowship. Seema and Gulzar are SWAN fellows and we thank them for their inputs.

EngageMedia.org/Pandemic-Control