DATA JUSTICE AND COVID-19: GLOBAL PERSPECTIVES

MEATSPACE PRESS

Edited by:
Linnet Taylor,
Gargi Sharma,
Aaron Martin, and
Shazade Jameson

DATA JUSTICE AND COVID-19:

GLOBAL PERSPECTIVES

Data Justice and COVID-19: Global Perspectives
Edited by: Linnet Taylor, Gargi Sharma, Aaron Martin, and Shazade Jameson

Publisher: Meatspace Press (London, 2020)
Weblink: meatspacepress.com
Design and illustrations: Carlos Romo-Melgar and John Philip Sage
Copy editor: David Sutcliffe
Format: Paperback and pdf
Printed by: Petit, Lublin
Paper: Splendorlux Versus Orange 250gsm and Arena Natural Bulk 90gsm
Set in: Lausanne by Nizar Kazan and Quarantina by Héloïse d'Almeida
Collage sources: ThisPersonDoesNotExist by Philip Wang and CCTV footage
Length: 304 Pages
Language: English
Product code: MSP08201
ISBN (paperback): 978-1-913824-00-6
ISBN (pdf, e-book): 978-1-913824-01-3

Contributors (alphabetically): Ramiro Alvarez Ugarte, Naomi Appelman, Lilana Arroyo Moliner, István Böröcz, Magda Brewczyńska, Julienne Chen, Julie E. Cohen, Arely Cruz-Santiago, Angela Daly, Marisa Duarte, Lilian Edwards, Helen Eenmaa-Dimitrieva, Rafael Evangelista, Ronan Ó Fathaigh, Rodrigo Firmino, Alison Gillwald, Joris van Hoboken, Shazade Jameson, Fleur Johns, (Sarah) Hye Jung Kim, Dragana Kaurin, Mika Kerttunen, Os Keyes, Rob Kitchin, Bojana Kostic, Danilo Krivokapic, Vino Lucero, Enric Luján, Vidushi Marda, Aaron Martin, Sean Martin McDonald, Silvia Mollicchi, David Murakami Wood, Francesca Musiani, Grace Mutung'u, Daniel Mwesigwa, Smith Oduro-Marfo, Aidan Peppin, Bojan Perkov, Andrej Petrovski, Ate Poorthuis, Gabriella Razzano, Andrew Rens, Cansu Safak, Kristin Bergtora Sandvik, Raya Sharbain, Gargi Sharma, Linnet Taylor, Eneken Tikk, Jill Toh, Anri van der Spuy, Michael Veale, Ben Wagner, Tom Walker, Wayne W. Wang (pseudonym), Bianca Wylie, Karen Yeung, (Melissa) Hye Shun Yoon, and two anonymous authors.

DATA JUSTICE AND COVID-19:

GLOBAL PERSPECTIVES

INTRODUCTION

COMMENTARIES

DISPATCHES

WHAT DOES THE COVID-19 RESPONSE MEAN FOR

GLOBAL DATA JUSTICE?

Linnet Taylor, Gargi Sharma, Aaron Martin, and Shazade Jameson

This book is a product of an exceptional moment in the evolving relations between technology, power, and justice. In early 2020, as the COVID-19 pandemic swept the world and states of emergency were declared by one country after another, the global technology sector—already equipped with unprecedented wealth, power, and influence—mobilised to seize the opportunity. This collection is an account of what happened next. The story these essays tell took place in the first months of the COVID-19 pandemic, capturing the emergent conflicts and responses around the world. The essays also provide a global perspective on the implications of these conflicts and responses for justice: they make it possible to compare how the intersection of

 state and corporate power—and the way that power is targeted and exercised—confronts, and invites resistance from, civil society in countries worldwide.

The collection consists of two main sections: commentaries and dispatches. We first invited authors from different countries, cross-border communities, regions, and sectors to write dispatches, which provide a point-in-time and local reflection on the role that data, technology, and industry are playing in the COVID-19 response. The dispatches come from every continent with confirmed cases of the virus, to permit a comparative analysis. We then made the dispatches available to a second group of authors who commented on emergent themes. We present these thematic commentaries first.

The global spread of countries included here reflects the unfolding of the first wave of the pandemic and must be understood in that context. For instance, it does not consider the connections between pandemic responses, data, and the Black Lives Matter protests, which unfolded as a result of this first wave. We should expect these connections to become the focus of scholarship by data justice researchers around the world in the coming months.

We initiated this collection, in part, because the pandemic has amplified a nascent *epidemiological turn in digital surveillance*. We have observed at least two dimensions to this turn: function creep and market-making. In the first, governments and technology vendors have pushed the repurposing of existing systems to track, predict, and influence. Much of this builds on techniques previously developed by mobile network operators for epidemiological surveillance in low and middle-income countries over the last decades. These efforts have previously been pursued in the name of both development[1] and humanitarian aid,[2] and are now being repackaged into proposals for the COVID-19 response.[3]

1
2
3

In the second dimension, software developers around the world have launched mobile apps to support contact tracing. Given that it appears that, at least in some cases, developers stand to benefit commercially from the use of these apps,[4] we also believe it is worth exploring the linkages between digital contact tracing and surveillance capitalism—the process of extracting value from data created as a byproduct of people's use of digital technologies.

4

Many contributors to this volume are academics, though we have also included

 civil society experts and journalists from around the world with a critical eye for the sociopolitical implications of technological and data-driven innovation. They have different and often contrasting views on how the use of data technology is being (or how it should be) pursued under the conditions of a global pandemic. Our contributors also bring with them different understandings of justice. As editors, we did not aim for consensus. This is the assumption at the centre of our work on global data justice: people perceive similar technologies and interventions differently depending on their standpoint, and we need to compare and contextualise their views to understand what common ideas of just data governance exist.

The questions we asked our contributors as a starting point for their essays were the following: What effects is the current global state of emergency having on the relationship between technology and authority? Are we seeing new trends? A different scale or acceleration of existing trends? What is the effect of the intensity of global attention to the emergency? Who are the points of articulation or facilitating actors for these developments? And who are the winners and losers in these changes?

The first-wave countries have demonstrated how politics and epidemiology intersect with pandemic technology development and data collection. Brazil, the US, and the UK, along with many lower-income countries, have all shown how the pandemic heavily penalises poverty, marginalisation, and invisibility, and that technology does not solve any of these in the absence of broader moves to provide justice. Developments in the UK are mentioned in several essays, likely owing to the fact that it is one of the jurisdictions in the English-speaking world where a contact-tracing app is being developed, spatial distancing guidelines have been resisted and debated in the public eye, and there has been an absence of pledges to resource an under-funded public healthcare system—a gap technology firms have eagerly offered their services to fill.

Our intended audience is diverse. This book can be read as a guide to the landscape of pandemic technology, but it can also be used to compare and contrast individual country strategies. We hope that it will prove useful as a tool for teaching and learning in various academic and applied disciplines, but also as a reference point for activists and analysts interested in issues of data governance, including data protection in emergencies, function creep, techno-solutionism,

technology theatre (i.e. focusing public attention on elaborate, ineffective procedures to mask the absence of a solution to a complex problem),[5] crisis entrepreneurialism, public–private partnerships, and questions of what constitutes legitimate intervention.

At first sight this collection might look as if it is making a case for technological exceptionalism—the idea that technology, and now data technologies in particular, occupy a unique position in society and that we should analyse their contributions and problems as a category of their own. Instead, the essays that follow demonstrate that data technologies both reflect and construct justice and injustice in ways that can be understood through analytical lenses we already possess. The pandemic has amplified many existing problems of technology and justice—including techno-solutionism; the frequent thinness of the legitimacy of technological intervention; excessive public attention on elaborate yet ineffective procedures in the absence of a nuanced political response; and the (re)production of power and information asymmetries through new applications of technology.

The questions raised by the following essays tackle these problems by interrogating both COVID-19 technologies and the political,

legal, and regulatory structures that determine how they are applied. The essays suggest that multiple factors influence how these technologies are experienced. Accountability, solidarity, rhetorics of collectivism, the need to signal belonging, and perhaps most importantly, perceptions of individual risk and potential advantage all play a role in how people respond to the request (or demand) that they engage with a particular application or intervention.

In particular, our contributors examine and test the link between the state of emergency and the use of power: Does the application of new monitoring and analytic technologies change relations of power between authorities and people, or merely amplify existing relations? What inequalities does the application of new, or repurposed technologies, make visible? And what responses do we see in terms of solidarity, cooperation or resistance? The way technology is being used in response to the pandemic reveals the relationship between authorities and citizen, how the public good is conceptualised in times of crisis, and how much accountability exists for the powerful. This book exposes the workings of state technological power to critical assessment—and, we hope, contestation.

Acknowledgements

This book was created rapidly in a moment of extraordinary disruption and anxiety worldwide. We would like to thank the contributors for their commitment to the project and for working under extraordinary time constraints, as well as the publisher and designers for putting the book together much faster than would normally be possible. We also want to acknowledge the many voices that are missing from this collection, including the many possible contributions that the pressures of the pandemic prevented from materialising. For this reason, we aim to keep expanding the collection through the Global Data Justice project[6].

References

1. Taylor, L. (2016) "The ethics of big data as a public good: which public? Whose good?" *Phil. Trans. R. Soc.* A.37420160126.

2. Including, for example, the Data for Refugees initiative: https://d4r.turktelekom.com.tr

3. See, for example: Oliver et al. (2020) Mobile phone data for informing public health actions across the COVID-19 pandemic life cycle. Science Advances 6(23).

4. See: https://www.wsj.com/articles/why-google-and-apple-stores-had-a-covid-19-app-with-ads-11591365499

5. See McDonald's commentary in the next chapter.

6. See: https://globaldatajustice.org

Linnet Taylor is an associate professor at the Tilburg Institute for Law, Technology and Society (TILT) in the Netherlands. She leads the ERC Global Data Justice project on data governance, representation, and social justice.

Gargi Sharma is a junior researcher at TILT.

Aaron Martin is a postdoctoral researcher on the Global Data Justice project at TILT.

Shazade Jameson is a social science researcher specialising in digital governance and smart urbanism, and a PhD researcher on the Global Data Justice project at TILT.

The Global Data Justice team worked on this project with funding from the European Research Council under the European Union's Horizon 2020 research and innovation programme (Grant Agreement n° 757247).


TECHNOLOGY
CHNOLOGY
THEATRE

AND SEIZURE

Sean Martin McDonald

This volume is hard to read.

The writing is beautiful, the analysis, sharp—but it's difficult to watch each author painstakingly document, prove, and predict the ways their cultures and politics are confronting the inequality embedded in their societies. Each piece is individual, but the trends are clear: Politicians are using the pandemic to, in some cases radically, redistribute power to serve their interests.

Nearly every dispatch points to expanding surveillance powers through COVID-19 apps, some highlight the ways that neutralised publics are unable to protect or preserve political opposition, and others recognise that, as in Hungary, barely restrained authoritarians are breaking completely free. In response to COVID-19, 84 countries have now declared domestic emergencies—and nearly all governments have exerted exceptional powers. The difference between the countries that have managed to minimise deaths and those unable to contain them is not power, money or even might—it is the trust of the governed.

Trust, like COVID-19, is a great equaliser. What too many governance experts forget is that you cannot legislate or force trust, any more than you can will the pandemic to end. Democracy, when it works, is a way to maintain and grow trust—it cannot manufacture or mandate it.

A number of the dead canaries pulled from the coal mine of our global trust crisis chirped to death over the role of technology. Edelman, the public relations firm behind the Trust Barometer, an annual global survey of public trust in institutions, has documented a steady downward spiral
1 across categories and geographies for years.[1] And a number of powerful books and articles have reflected on the relationship between digitisation, automation, and the legitimacy of the public services that employ them. In the 2014 outbreak of Ebola in West Africa—the 20th outbreak
2 of Ebola in the region[2]—the biggest driver of spread was not the virus *per se*, it was that it struck in areas that lacked credible leadership.

The true legitimacy test for any government is whether it can convince its people to do something difficult, together. The COVID-19 response requires us to make large changes to the way we do almost everything—and we have to hold those new stances, without fail, for an indeterminate period. Together.

As many of the analyses in this collection illustrate, COVID-19 has exposed just how divided a number of societies are, both internally and with respect to the rest of the world. While technology is only one of the structural inequalities that limit the effectiveness of COVID-19 response efforts, the universal risk posed by the virus means that any app-based approach is an inequitable and marginal intervention, at best. The inability of technology to make COVID-19 legible to us, even granted nearly unrestrained invasion into our daily lives, should serve as a stark reminder of the tremendous inequities embedded by digital-first government. An unfortunately small amount of the press coverage of COVID-19 response technologies confronts those divides, nor their impact. To their credit, the earliest adopters of digital contact-tracing apps—the poster child for COVID-19 technology—have been transparent about their effectiveness. The leads of nearly every major digital contact tracing deployment have been clear that the apps have made little-to-no difference in tackling the spread of the virus, and in Israel, public health authorities have said
3 they have been actively detrimental to the response.[3]

There have, of course, been a number of surveys of public trust, debates about data architecture versus privacy rights, and digital epidemiologists' campaigns for a cure. The one thing they all have in common is that where they are the loudest, the death toll is rising.

Technology Theatre

The intersection of technology and politics is religious—everyone has important, valid beliefs—and nearly all the systems we have for exerting them are complex at best, and quite often exploitative. Like religion, most of the important decision-making happens behind closed doors, while the implicit benefits are made performatively and theatrically accessible to the public. And, like religion, there are a lot of benefits—especially for those willing to conform—but they, too, are complex and open to a lot of exploitation. This volume details an enormous number of these theatrics; which are unique in context, but common in tactic and structure.

Put simply, the instrumentation of governmentally deployed technologies is being used to distract the public from the political impacts of their use. I call this Technology Theatre, in the tradition of Bruce Schneier's Security Theatre,[4] referring to the practice of focusing public attention on elaborate, ineffective procedures to mask the absence of a solution to a complex problem. Bruce Schneier is a digital security specialist, but the most prominent examples of security theatre usually involve high volumes of low-fidelity inconveniences, like liquid bans and shoe removal requirements in airports. The point of security theatre is to get you to focus on the inconvenience of the process, so that you don't spend any time interrogating whether those measures have any meaningful impact on solving a real problem.

4

Technology theatre is similar, and on full display in the COVID-19 response—most acutely in the debate around contact tracing technologies. As illustrated throughout this volume, and in the significant amount of mainstream media coverage during the early stages of the COVID-19 epidemic, governments and companies all over the world are focusing conversations on what proximity-tracking protocol is being used by apps (e.g. Bluetooth, telecom databases, GIS) and

the appropriate centralization and privacy of the underlying data sharing relationships. Never mind that the head of every major 'successful' contact-tracing app deployment has said the technology added little-to-nothing, where it didn't actively harm public faith in the health response—as seen in Israel, the UK, Australia, and Austria, among others. The idea that an app based on our experimental (at best) understanding of COVID-19, would bridge the gap between under-resourced and politically intransigent leadership and the delicate, difficult requirements of an effective, sustained response effort is fantasy—albeit a politically and commercially useful one. Here, there aren't many good-faith arguments that contact tracing apps deserve any attention, let alone public deployment—but the show must go on.

Make no mistake, there are complex problems at play in this pandemic, but more of them are a product of governmental failures than of COVID-19 itself.

Seizure

The deployment of a technology is a proxy for a seizure of power. In private markets, we allow that seizure because it is not mandatory, so any adoption is taken as an indication that the person using it finds the exchange fair. In public systems, we expect government officials to deploy those tools only with a valid mandate, and within whatever domestic checks and balances underpin the institutions' legitimacy. The vast majority of public governance bodies, from legislatures to tax authorities to regulatory certification bodies, have struggled to deliver either of these models of checks on the technology industry, even without a public health emergency.

During emergencies, we typically suspend a number of the checks placed on public authorities, and often limit or reduce the function of administrative agencies, like market regulators and consumer protection advocates. Emergencies are the perfect storm for exploitation, especially those that serve public and political ends—as described by Naomi Klein in *The Shock Doctrine*.[5] The technology industry fully realises this opportunity. It is reporting record profits amidst a historic recession in nearly all other sectors. And it is not just because many are stuck

at home streaming movies. When companies spend money developing the capacity and tools to perform any function, they have to demonstrate a business logic for them. The technology we built for surveillance yesterday has been retooled and redeployed for COVID-19 biosurveillance and, based on its need for more capital, the industry will remarket and ratchet those same capacities during the next crisis.

Unlike technologies, though, emergency powers were designed to be temporary—and accountable. Most forms of emergency powers require that when a government infringes on your rights, they owe you redress, even if that redress is delayed. For example, most forms of eminent domain, a government's right to seize a property during an emergency, require the government to pay you the fair market value of the property. Mileage varies in implementation, obviously, but the point remains: democracies do not allow seizure without accountability or restitution. Most emergency powers are also subject to periodic review, with no guarantee of renewal, either by a legislature or the lead justice advocate. And while it is easy to delete an app, it can take years to stop insurers incentivising employers to require it of workers. As this volume illustrates, there will be an enormous number of individual contexts and outcomes when we start trying to force biosurveillance and proximity tracking apps back out of our lives, long after we have pressed delete.

COVID-19 is just a pathogen. The response of our leaders, however, has revealed a body politic that is sclerotic, weak, and immunosuppressed. Our tendency to focus on the instrumentation of technologies, instead of the seizures of power they represent, is orchestrated—and it is not the first time this has happened. No government should be relying on an app architecture to protect a public from itself. One of the primary values of public, independent governance is that, when it works, we are able to focus on—and participate in—solving the problems of our era, together. The governance of technology, and its growing role in our public institutions and lives, is one of those problems which, as this volume amply shows, has only accelerated in the COVID-19 response. Now, it is *the* problem—and many of us, it seems, will have to try to solve it without government.

26 Thankfully for the health of our publics, as this volume also shows, there are a number of clinicians focused on the pathway to cure.

References

1. See: https://www.edelman.com/trustbarometer

2. See: https://www.cdc.gov/vhf/ebola/history/chronology.html#anchor_1526565058132

3. For Singapore, see: https://jamanetwork.com/journals/jama/fullarticle/2765252; for Iceland, see: https://www.technologyreview.com/2020/05/11/1001541/iceland-rakning-c19-covid-contact-tracing; for Israel, see: https://www.haaretz.com/israel-news/.premium-israeli-doctors-warn-shin-bet-surveillance-hindering-efforts-to-combat-coronavirus-1.8714359; and broadly: https://www.wired.co.uk/article/contact-tracing-apps-coronavirus

4. See: https://www.schneier.com/essays/archives/2009/11/beyond_security_thea.html

5. Klein, N. (2007) *The shock doctrine: The rise of disaster capitalism*. London: Penguin.

Sean Martin McDonald is a senior fellow at the Centre for International Governance Innovation. He is the author of Ebola: A Big Data Disaster.

PAPERING OVER THE CRACKS:

ON PRIVACY VERSUS HEALTH

Vidushi Marda

Technological solutions to COVID-19 have reignited a conversation about the relationship between privacy and public health. As contact-tracing apps (see chapter by Kitchin), large-scale data analytics (see chapter by Wang), and repurposing of old technologies for new uses (see chapter by Cruz-Santiago) gain traction, the relationship between privacy and health is being framed as a choice. This is an oversimplification at best, and a distraction at worst.

An oversimplification, because it assumes that limitations on privacy are a binary, i.e. privacy can either be absolutely guaranteed or non-existent. This is not the case. The fundamental right to privacy is recognised under international human rights law, and many (though not all) national legal frameworks. It is not, however, an absolute right. It can be subject to reasonable and proportionate restrictions that are strictly and narrowly defined under international law. The (similarly) false dichotomy of privacy versus health ignores these established legal standards when it pushes for unfettered surveillance and executive power in the name of emergency response (see chapter by Eenmaa Dimitrieva et al.). It cloaks

the pandemic response with unjustified exceptionalism—while laying the groundwork for infrastructures that will continue to violate privacy well after the pandemic has passed.

Arguments about privacy versus health are also a distraction, or at least not unique to the current situation: because privacy concerns, while obviously crucial amidst the current crisis, are merely reflective of a much deeper issue stemming from the uncritical adoption of technological solutions to social problems. Implicit to this adoption is an acceptance of the institutional, structural and governmental status quo—wilfully ignoring the deficiencies that have led to (for example) inadequate pandemic responses in the first place.

Increasing reliance on public–private partnerships

Public–private partnerships are a focal point for most tech-based solutions. As states usher in privately developed technology at the cost of due process (see chapter on Canada by Wylie), an unlawful erosion of fundamental rights seems almost inevitable, as the actors that bring these technologies into existence do not need to meaningfully reckon with the legal safeguards or freedoms they dilute. This is for a number of reasons. First, fundamental rights and corresponding safeguards assume a vertical relationship between the state and the individual, and don't neatly provide for their horizontal application, i.e. enforcement against private actors. Further, privately developed technology is often brought into governance contracts through opaque processes that concern governments and private actors alone, and do not lend themselves to transparency, accountability, public consultation, and legal oversight.

With the promise of sophisticated emerging technology, private actors are provided the space to rely on the hoped-for potential of these technologies, instead of having to justify their use given known limitations and dangers. For instance, consider the UK government's partnership with Palantir to predict surges in NHS demands during the pandemic.[1] Reports have already begun to emerge that the service could be continued even after the current health emergency, provided that Palantir is willing to supply it at less than the market rate.[2] Despite this, details of the partnership

(monetary, substantive or legal) are still unknown, and Freedom of Information Act requests have gone unanswered (see chapter on the United Kingdom by Mollicchi et al.). This systemic and systematic privatisation of governance perpetuates the dilution of rights because it also involves a grave misalignment of incentives: private actors in the business of building technology are bound to push for technological solutions, greater data collection and access, and have ample motivation to overplay the benefits of technology in the realm of governance.

Sidestepping critical reform of power and institutions

When technology is presented as a scalable and efficient solution to complex social problems by governments, companies, or (more often than not) a combination of the two, there is little (if any) space to question the power structures and institutions that gave birth to these social problems in the first place. Technological solutions like contact-tracing apps, for instance, can optimise for and facilitate the functioning of existing structures of law enforcement and healthcare, but won't necessarily acknowledge the underlying inequalities of the societies in which they will function, or the broken healthcare systems and/or discriminatory law enforcement forces that could use and wield them.

This narrow approach is misguided, as the societal and institutional reality within which sociotechnical systems come to be developed and used are a crucial piece of the deployment puzzle. For instance, contact tracing apps require a minimum uptake to be effective, and yet deployments in at least some jurisdictions have failed to consider the stark digital divides (see chapter on Jordan by Sharbain and Anonymous) that could preclude effective outcomes.

This approach is also actively harmful, as these technologies have a disproportionate impact on marginalised groups and minorities, due to heightened risk of surveillance, or vulnerable groups being targeted by law enforcement authorities steeped in historical and societal biases against them. For instance, Palantir's Gotham software has been directly linked to human rights violations against immigrant families by the United States Department of Homeland

Security,[3] and yet, Gotham, along with a newer Palantir software called Foundry, is currently being used as part of the COVID-19 response in the UK (see chapter by Mollicchi et. al) and Germany (see chapter by Wagner).

3

The false dichotomy between privacy and health, therefore, feels particularly nefarious. It represents an implicit resignation to current infrastructures, accountability frameworks and institutions, and side-tracks questions around funding, politics, and healthcare. This false dichotomy encourages situations where facial recognition is used by law enforcement to ensure that social distancing norms are complied with, for instance, while skirting the question of why social distancing is a luxury that large parts of society do not have. It allows for situations where private players and governments have a plethora of options for using and repurpose sensitive personal data, without meaningfully questioning the premise and extent of data collection in the first place.

Most technological solutions developed in response to COVID-19 are primed for mission creep: built in a hurry, shrouded by secret contracts, and rolled out in the absence of redress mechanisms or legal safeguards. Data protection safeguards are thus a crucial first step in tackling a larger and more layered issue—but they will not prevent a repetition of similar problems in the future if they are isolated from the need for overall structural reform.

Technological responses to COVID-19 have crystallised in the public eye the profoundly shallow ways in which we are led to tackle emergency situations. The infrastructures being built and sold under the umbrella of pandemic response arise from a technocratic tendency that predates COVID-19, and will endure much longer than the current situation. This inadequacy of technological solutions will simply be entrenched around the next crisis—whatever it is—unless there is less glamorous, but infinitely more important, work done on rethinking institutions, structural inequality, funding, and discrimination. Outsourcing fundamental aspects of governance to private companies or technology just sets us up to fail—further fracturing a system that is already broken.

References

1. See: https://tech.newstatesman.com/coronavirus/palantir-45-engineers-to-nhs-covid-19-datastore and https://healthtech.blog.gov.uk/2020/03/28/the-power-of-data-in-a-pandemic

2. See: https://tech.newstatesman.com/coronavirus/palantir-covid19-datastore-coronavirus

3. See: https://www.vice.com/en_us/article/ywadv7/ice-just-renewed-its-contract-with-palantir

Vidushi Marda is a lawyer based in Bangalore, India.
She currently works as senior programme officer at Article 19.

SOVEREIGNTY
SOVEREIGNTY,
PRIVACY
AND

CONTACT TRACING PROTOCOL PROTOCOLS

Michael Veale

Bluetooth-based COVID-19 contact-tracing apps became an international meme in early 2020. As the crisis headed from epidemic to pandemic, I joined an international consortium of researchers who were concerned about the potential for misuse, mission creep, and abuse of these new infrastructures. Our intervention was to create a decentralised open protocol and codebase called Decentralised Privacy-Preserving Proximity Tracing (DP-3T). It used cryptographic methods to enable smartphone owners to be notified if they had a significant contact event (insofar as Bluetooth can detect it) with a later diagnosed individual, but without requiring a centralised database or persistent identifiers. In contrast, centralised systems, such as Singapore's early *TraceTogether* app, effectively broadcast an ID card that only the state can read, centralising a social graph of physical interaction by requiring diagnosed individuals to upload

data about other people's co-location. DP-3T removed this centralised database to limit data repurposing beyond public health, and removed persistent identifiers to limit function creep towards quarantine control or 'immunity certificates.'

The DP-3T project, then featuring eight universities, was initially part of a pan-European consortium set up in response to COVID-19 called Pan European Privacy-Preserving Proximity Tracing (PEPP-PT), which intended to develop privacy-preserving contact tracing as a partnership between academia and industry. Over time we became increasingly frustrated with PEPP-PT's industrial leadership pushing centralised approaches to governments behind closed doors, using our team's academic credibility to do so, which concerned us. We published the DP-3T protocol in early April for discussion and feedback, but it soon became apparent that PEPP-PT was building a Trojan horse: using the privacy community's wide approval of our public system to slip their own, unpublished centralised approach into deployment. DP-3T universities resigned from PEPP-PT, and despite hiring several crisis PR firms in response (including the German firm notable for its work for Volkswagen in *Dieselgate*), the consortium eventually collapsed.

In parallel, the tech giants entered the scene.

All state-sponsored COVID-19 apps are de facto public–private partnerships between a government, Apple, and Google. Effective enclosure has meant software can only run on the firms' devices with their blessing. Papal levels of blessing are required if unusual sensor access is desired, and the Bluetooth access needed for contact tracing is unusual. Apple typically restricts the use of Bluetooth when apps are off-screen ('backgrounded') through a mixture of software and App Store 'soft law' in order to limit covert, commercial tracking. Apps based on Singapore's *TraceTogether* required problematic technical workarounds. iPhone users had to leave the app open, phone screen on, and unlocked in their pockets as they went about their daily business. This was an inconvenient, insecure, and damaging requirement, crippling participation rates.

In a surprising partnership, Apple and Google announced a system that became known as Exposure Notification on April 10, 2020. This system allowed apps made by national public health authorities to use Bluetooth in the background, although with conditions. Background Bluetooth use was conditional on use of the new Exposure Notification API (instead of the regular code needed to call Bluetooth from apps). This code, explicitly stated by the firms as based on DP-3T, was buried at the operating system level. Importantly, it was deliberately missing a building block that centralised systems would need: it did not allow the app to obtain a list of all identifiers the phone has seen. Centralised apps need these, as they rely on diagnosed people uploading the identifiers of others they have been close to. Decentralised apps, however, only ever transmit information upon diagnosis that an individual's device emitted; the identifiers relating to others that a device heard never need to leave it. This was a conscious move: the firms—or at least Apple, whose operating system was the main impediment to Bluetooth use—would not permit centralisation of data.

A PR-friendly narrative for the firms' actions would state that, pressured around the world and with time constraints to match, they had to engineer a system for a country with minimal legal privacy protections in mind. The European Parliament had indeed demanded decentralisation in a resolution on April 17, 2020, and the European Data Protection Board had also expressed this preference. Building these restrictions into code, rather than the 'soft law' of what can be accepted into the App or Play Stores, would bind their own hands more successfully against government pressure, as a secure operating system update relating to increasing functionality of core sensors is not a quick task.

The consequences of this decision go beyond that, however. Centralised and decentralised proximity tracing systems are largely incompatible. To open up Europe's closed borders, interoperability became high on the agenda. A mass of centralised systems creates coercive pressure for centralisation, and vice versa. Before long, Germany, Switzerland, Estonia, Italy, and many more countries had designed and/or deployed systems based on DP-3T,

Exposure Notification, or both. At the time of writing in June 2020, interoperability was in an advanced state of discussion. Removing friction within a walled garden rather than with outside it, is, of course, straight out of the classic platform playbook.

Some states, notably France, were furious at Apple's decision, declaring it to be an attack on their sovereignty. France wanted a centralised system, stating a desire to mitigate a particular niche snooping attack possible for a tech-savvy neighbour, which affects all Bluetooth contact tracing systems to some degree. NHSX, the tech branch of NHS England, wanted centralisation to experiment with fraud detection, given that a lack of speedy tests in the country meant they wished for an app to allow for abuse-prone self-reporting rather than only test-based diagnosis. Oddly, it is notable that there has been little appetite to attempt to rectify this situation with the legal obligations that sovereign states have at their disposal; instead reifying the view of tech giants as state-like themselves, diplomatic interlocutors rather than firms operating under national law. Sovereignty was mourned before any of its traditional tools were even reached for. Privacy researchers by and large cautiously welcomed the Apple–Google partnership as it provided assurances over short-term COVID-19 surveillance and centralised data breach concerns, but were rightly wary of the obviously unchecked—and potentially uncheckable—power of these platforms.

This ongoing saga highlights the need to think of new ways to control platform power in years to come. While in DP-3T we built a tool that preserved confidentiality, this does not mean it doesn't wield power, or that it sidesteps issues of justice. Google, for example, has been experimenting with federated learning in the Chrome browser—where separate personalisation or targeting algorithms are built for each person without much or any data leaving an individual's device—and has toyed with abolishing third-party cookies. This would preserve confidentiality, but continue to allow firms to optimise, intermediate between, and manipulate populations very similarly to the ways they do currently. Individuals, communities, and governments have limited

power to control the code that runs on their devices, and by extension the protocols they participate in, while the designers of privacy-preserving technologies typically (and strangely) build systems with the assumption that they retain the right to refuse software. To change the status quo of global systems governed by global firms is to open Pandora's box. Both the chance for individuals to escape platform power, but also the chance for states to demand changes such as the abolition of end-to-end encryption, might lurk inside. The drama of contact tracing applications has laid bare how much of both extractive *and* protective infrastructure is reliant on the choices of a small number of gargantuan corporations. A surprising legacy of COVID-19 might be the new visibility of these protocol politics to politicians, who may yet decide to shake up the situation in the years to come, with consequences that remain hard to anticipate.

Michael Veale is lecturer in digital rights and regulation at University College London. He is a co-author of the decentralised Bluetooth proximity tracing protocol, DP-3T.

APPS, POLITICS, AND POWER: PROTECTING RIGHTS WITH

LEGAL AND SOFTWARE CODE

Lilian Edwards

In the current global pandemic, policy interest has alighted on 'contact-tracing apps', programs downloaded to smartphones, which digitise and speed up long-established manual practices of contact tracing, testing, and isolating for control of infection. There has been a flurry of such digital tools proposed all over the world, motivated by early apparent success in countries like South Korea, Singapore, and Taiwan.[1] One problem with the COVID-19 virus is that it is highly infectious in a period of up to seven days before symptoms show. As a result, contacts arguably can't be alerted speedily enough by conventional manual tracing, which obviously only starts after symptoms develop. Another issue is that traditional contact tracing is limited by the fact contacts might not be recalled or may be strangers unknown to the infected person. Apps that measured proximity and time of contact between persons were ballyhooed as the technical answer to both problems.

1

Initial enthusiasm for contact-tracing apps has been tempered, however, by two key worries: privacy and efficacy. Apps had originally gained traction in Asia,

where Western common myth has it that privacy is of relatively little concern either because of lack of emphasis in authoritarian regimes or, even in democracies, due to relatively little history of strong privacy rights. In fact, it is more likely that by the accounts of Asian scholars themselves, apps were more acceptable due to a higher degree of trust in, and appetite for, technological solutions. In Europe, however, trust is low,[2] and privacy considerations are seen as vital because they might further impair confidence and prevent people from downloading and using a contact-tracing app. Research had shown that for full efficacy, around 80% of the smartphone-owning population has to download and use the app,[3] so confidence was vital given the assumptions of voluntary—not mandated—uptake. The use of Bluetooth Low Energy (BLE) to trace proximity between persons (or rather their phones) as pioneered by Singapore, rather than GPS location, both promised to increase accuracy and reduce privacy worries, but arguably not enough.

The privacy issue became the centre of a heated debate over how to build contact-tracing apps; that is, whether they should adopt a 'centralised' or 'decentralised' strategy. In the former, some personal, albeit generally pseudonymised, data about the social contacts of infected persons is stored centrally. The proposed advantage of this is that it allows centralised 'risk scoring' and hence fewer false alerts that make contacts isolate needlessly—even where, as in the UK, contact tracing was initially to be based on self-reported symptoms rather than confirmed positive test results.[4] In 'decentralised' apps however, no or minimal personal data is gathered, as proximity data is stored locally on phones rather than being made accessible to the state. Mass surveillance via the app beyond the immediate emergency thus looks in principle impossible.

In the UK, NHSX, the recently conceived digital wing of the NHS, began building an app in the relatively early days of the pandemic, in March 2020, and trials began on the Isle of Wight on May 5, 2020.[5] However, despite early plans to have the app out by mid-May,[6] the app was repeatedly delayed by troubles hit during the testing period. Meanwhile

global events overtook it. On April 10, Apple and Google in an unprecedented joint move announced that they would collaborate to offer a decentralised protocol to states, so such apps could be built more efficiently for Android and Apple phones.[7] The soft power of their stranglehold on the smartphone market led to almost every country in Europe except France and the UK adopting (or in Germany and Norway's case, switching to)[8] the new 'Gapple' approach.[9] After mounting pressure from other countries' trajectories, the media and academics, on June 18, 2020 the existing centralised app was essentially dumped by NHSX and efforts switched towards investigating if a new app based on the Gapple protocol would work better. It still seems quite plausible that the UK may choose in the end to have no app at all, despite lack of confidence in its equally troubled 'track and trace' manual tracing strategy.[10]

While the Gapple API has emerged as the winner of the privacy wars, it is not a fix for all societal ills. It focuses attention on privacy-preserving architectures as technological cure-alls, at the expense of investigating the wider legal, ethical, and social context in which any app will be implemented. It ignores *how* any app will be used, especially given the imperative towards high uptake, combined with known demographics of digital exclusion, poverty, and techno-illiteracy, not least among the old who would have the most to gain from control of the virus. What about those who do not have smartphones? Would people be compelled to install the app? Who could make them show what notifications they had had? The state, employers, those who ran spaces like shopping malls or sports stadiums? What sanctions might there be for non-use or non-display? What groups might suffer most harm and discrimination as a result? Who would provide oversight?

These problems were not merely applicable to the UK with its centralised app but applied to Gapple apps as well. However the UK has been particularly dogged in claiming that no new law was necessary to mitigate these possible abuses given already existing EU data protection law. While countries such as Italy, Belgium and Australia have passed specific laws or amendments guaranteeing rights after contact tracing

apps were implemented, the UK has pointedly refused to do such. Yet UK equality law is certainly not sufficient to prohibit discrimination on the basis of using an app,[11] nor on the basis of coronavirus status, and rights such as freedom of movement and autonomy are only in the most abstract sense protected by the Human Rights Act 1998 and its 'parent' the European Convention on Human Rights.

Accordingly, a team led by the author drafted a model Bill in early April 2020[12] which sought to propose key legal safeguards in relation to the NHSX app either not, or not stringently enough, covered by, current data protection law. The five main planks of the Bill were:

(1) *Digital exclusion*: No compulsion to own a smartphone
(2) *Non-coercion*: No compulsion to install or use an app, or to display data sent to or from the app to any party
(3) *Retention/deletion*: Personal data collected by apps must be deleted or securely anonymised within 28 days
(4) *Oversight*: a new Coronavirus Safeguarding Commissioner to review safeguards across the entirety of COVID-19 emergency laws
(5) *Immunity passports:* No discrimination on the basis of having, or not having, such a certificate unless justified by and proportionate to a public, legitimate goal

Such choices are not just about legal cohesion, but are political and contentious, especially (2) and (5). If social good requires maximum uptake of an app, can coercion not be justified? Anecdotally, it seems those groups already fearful of state surveillance—ethnic minorities, religious groups, and those anxious about immigration or self-employed status—are most likely to worry about installing the app; while those already disempowered in the workplace, such as gig workers, are most likely to suffer discrimination if apps are abused. In some jobs, refusing to install or display the app might give employers reasons to dismiss or exclude disliked workers or groups that

would otherwise be illegal. Compelling use of the app might fatally impair trust and encourage users to supply false and partial data as well as infringe their basic human rights.

We found that the issues became even more controversial as we looked at the future technology of so-called 'immunity passports'—the very purpose of which is to discriminate. Should law not prevent the happenstance implementation of what would effectively be a new digital ID card and internal passport? Our answer, drawn from human rights scrutiny, was not to ban the immunity passport *in toto*—given its social good of not only releasing some sections of society from emergency restraints on rights and freedoms, and also helping restart the economy—but to turn to legally familiar transparency, legitimacy, necessity, and proportionality tests. We felt uncertain in our choices, and it was affirming that legislatures such as Australia,[13] Switzerland[14] and Italy[15] had begun themselves to pass 'voluntary' and 'non-coercion' clauses in bespoke laws or amendments to existing law.

13, 14, 15

As of June 2020, the attempt to provide 'legal code' to safeguard the UK against abuse of a centralised app has been stymied and then sidelined. Despite support from the cross-party Joint Committee for Human Rights who drafted their own COVID-19 Safeguards Bill,[16] the UK government has remained firmly opposed to any new laws.[17] Speculatively, this might have been because parliamentary debate would have dangerously exposed the early failures in testing provision which led to the centralised app design adopted by NHSX, as well as the failure to pivot when testing became better available, and evidence accumulated that in practice non-Gapple apps would no longer work effectively on Apple phones.[18]

16

17

18

It is still quite likely that in many countries the uptake necessary to make apps useful will not be achieved, in which case, legal safeguards might at least prevent a damp squib technology from becoming an actively harmful vehicle for discrimination and future mass surveillance.[19] In the UK, the PR disaster of the U-turn on the centralised app makes allowing debate on a safeguards Bill even more unlikely, even if a new Gapple app does arise from the ashes.

19

By contrast, in civil law countries the idea that such an app needs a legal foundation seems to be becoming normalised. Much of this story—in the UK at least—has been about what decisions made out of political expediency can be justified later, and less about pure jurisprudential debates about the balance between public good and private rights. Framed globally, the story is about how sovereign power in nation states could be diverted by the soft technology power of the two most powerful technology companies on the planet. As we move into the post-lockdown era it is likely that severe problems will remain to be solved around the use of immunity passports for travel and the use of apps as workplace surveillance. What gaps in safeguards exist in these two areas is something all countries should be investigating to determine what safeguards for human rights are necessary and how they should be introduced.

References

1. The claim that contact-tracing apps alone were the foundation of these countries' success in fighting the virus has since been widely repelled. See: https://www.nature.com/articles/d41586-020-01264-1

2. Shortly before the centralised app was terminated, a study from the Reuters Institute for the Study of Journalism / Oxford Internet Institute showed that of a cohort signed up to receive news about COVID-19, around 82% were prepared to wear a face mask but less than 50% would download the app. See https://reutersinstitute.politics.ox.ac.uk/even-low-news-users-say-they-are-willing-take-preventive-measures-against-covid-19

3. See: https://www.research.ox.ac.uk/Article/2020-04-16-digital-contact-tracing-can-slow-or-even-stop-coronavirus-transmission-and-ease-us-out-of-lockdown According to the Ofcom figures, 20% of the UK population do not own a smartphone, so this figure becomes around 60% of the total population. In later government pronouncements, this figure mysteriously shrunk to 50%.

4. Epidemiological advantages such as the identification of recurrent viral 'hotspots' were also claimed because more data could be gathered than just pure proximity; however, such data can also be delivered voluntarily alongside a decentralised app. In fact, the UK app moved to alerting contacts based only on positive tests in version 2 of the app, which was due to be trialled in June 2020 but never was, due to the cancelling of the whole centralised app programme.

5. See: https://www.the-scientist.com/news-opinion/uk-launches-trial-of-contact-tracing-app-on-isle-of-wight-67516 ; https://www.bbc.co.uk/news/technology-52532435

6. During this time, the devolved parts of the UK which have control of their own health systems have also gone their own ways. Northern Ireland declared that they would build their own app which would be compatible with the decentralised model adopted by the Republic of Ireland (see chapter by Kitchin) and Scotland has yet to decide if it wants a contact-tracing app at all.

7. See: https://www.apple.com/uk/newsroom/2020/04/apple-and-google-partner-on-covid-19-contact-tracing-technology

8. See: https://uk.reuters.com/article/uk-health-coronavirus-europe-tech/germany-flips-to-apple-google-approach-on-smartphone-contact-tracing-idUKKCN22807X

9. It should be noted that the decentralised model was pioneered by the European academic DP3-T consortium, who were at least partially responsible for the Apple uptake. See: https://github.com/DP-3T/documents

10. See, for a timeline of the story, "Coronavirus: What went wrong with the UK's contact tracing app?", BBC News, 20 June 2020, at https://www.bbc.co.uk/news/technology-53114251

11. The Equality Act 2010 does not include health, and certainly not contagious disease status, as a protected characteristic. One suggestion of the Coronavirus Safeguards Bill was that COVID-19 status become a protected characteristic.

12. 'The Coronavirus (Safeguards) Bill 2020: Proposed protections for digital interventions and in relation to immunity certificates', lead drafter Lilian Edwards, Professor of Law, Innovation and Society, Newcastle Law School. A team assisted, including Michael Veale, Orla Lynskey, Rachel Coldicutt, Nóra Loideain, Frederike Kaltheuner, Marion Oswald, Rossana Ducato, Burkhard Schafer, Elizabeth Renieris, Aileen McHarg, and Elettra Bietti. See: https://osf.io/preprints/lawarxiv/yc6xu

13. Enacted in the temporary Biosecurity (Human Biosecurity Emergency) (Human Coronavirus with Pandemic Potential) (Emergency Requirements—Public Health Contact Information) Determination 2020; see now Privacy Amendment (Public Health Contact Information) Act 2020: https://www.legislation.gov.au/Details/C2020A00044

14. See report in English at http://www.loc.gov/law/foreign-news/article/switzerland-regulation-on-proximity-tracing-app-pilot-adopted ; the temporary Swiss regulation of 13 May 2020 is at: https://perma.cc/9MHZ-CC54

15. See: https://twitter.com/SilviaPetulante/status/126777515133413760 Liberty have also spoken out against coercion, see: https://www.theguardian.com/law/2020/apr/26/dont-coerce-public-over-coronavirus-contract-tracing-app-say-campaigners

16. See: https://www.parliament.uk/business/committees/committees-a-z/joint-select/human-rights-committee/news-parliament-2017/covid-contact-tracing-app-draft-bill-19-21

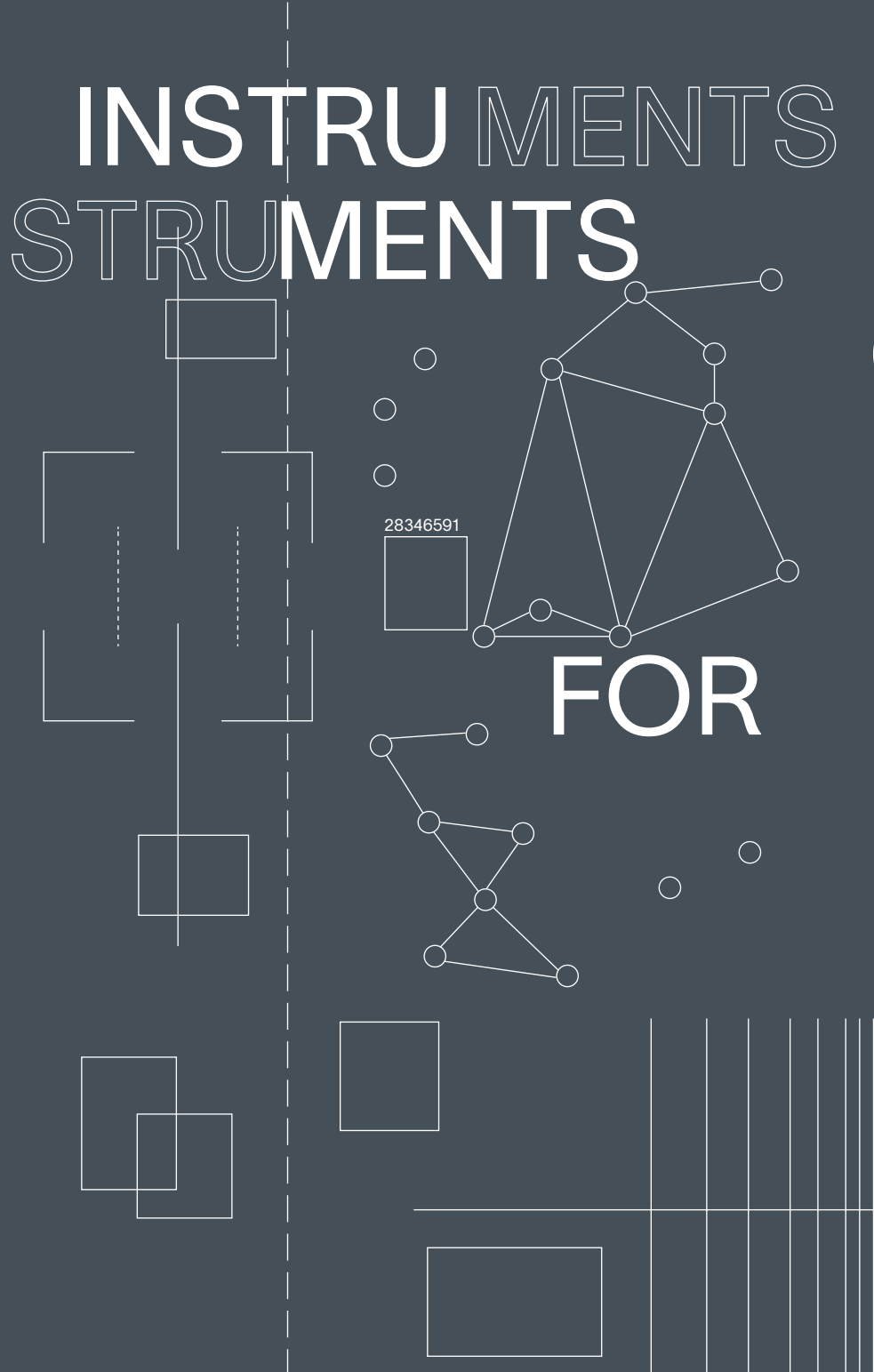
17. See: https://www.computerweekly.com/news/252483536/Hancock-to-Harman-No-contact-tracing-privacy-law

18. Baroness Dido Harding in charge of Track and Trace for the UK announced on 18 June that the nascent NHSX app would only detect contacts with 4% of Apple phones. This seems to have been the key point that led to the demise of the centralised app.

19. For example Australia, whose app was downloaded after a month by 6mn users and only resulted in the known tracking of one contact who was infected (https://twitter.com/grahamgreenleaf/status/1265132223549673472) See for background on their law, G Greenleaf "Australia's 'COVIDSafe App': An Experiment in Surveillance, Trust and Law" (2020) University of New South Wales Law Research Series 999.

Lilian Edwards is professor of law, innovation, and society at the School of Law, Newcastle University, United Kingdom.

INSTRUMENTS
STRUMENTS



FOR

PANDEMIC GOVERNANCE

Karen Yeung

Governing through a pandemic presents extraordinary challenges. It requires a complex blend of power, resources, expertise, leadership, and cooperation across society. Three tasks of particular importance are: devising a set of containment measures, continually gathering information about the impact of those measures and the needs and welfare of citizens over time, and determining which instruments to utilise. To date, the promulgation of lockdown orders and social distancing laws have been the most significant intervention, imposing extraordinary and unprecedented restrictions on the basic right to freedom of movement. Such measures can be understood as 'social' interventions because they rely critically on voluntary co-operation by the public. Even when mandated by law and backed by penalties for violation, the practical impossibility (at least in non-authoritarian states) of enforcing all infractions across a population means that it is not primarily a fear of the coercive power of the law that has been the primary motivation underpinning the compliant behaviour of citizens, but their willingness to 'do their civic duty' by choosing to comply with both the letter and spirit of the lockdown orders imposed upon them in the service of the greater good and the preservation of the lives of others.

52 Solidarity, sacrifice, and voluntary cooperation by citizens

Widespread compliance with lockdown rules reflects the strength and significance of individual and collective acts of social solidarity, which rely upon the trust of citizens in their governors and in each other, and which governments must actively seek to nurture and sustain if social interventions are to be effective. The price citizens have paid (and continue to pay) in their voluntary self-restraint are revealed in countless stories of love, loss, and separation as individuals everywhere make painful sacrifices, forgoing opportunities to be physically present with loved ones at critical moments. These personal sacrifices are acutely and devastatingly reflected in the experience of many thousands of individuals who have suffered and died alone without loved ones by their side because their families chose, with great sorrow and reluctance, to comply with lockdown orders. In the UK, the extent of those sacrifices was vividly illustrated by the extraordinary level of public fury directed at the Prime Minister's Special Advisor, Dominic Cummings, for his unapologetic violation of the spirit (if not the strict letter) of the lockdown rules during the height of the crisis. Although digital communication technologies have been essential lifelines during lockdown, the pandemic has exposed them as vastly inferior substitutes for embodied human interaction, reminding us that human relationships are nurtured and sustained by physical touch and the warming presence of those we love. By asking citizens to forgo these interactions, governments have determined that the need to minimise human contact in order to reduce the spread of the virus exceeds the value of those human interactions that have been ruled impermissible. These kinds of normative trade-offs cannot be determined by scientific evidence alone. To this end, the bluntness and stringency of UK lockdown rules have been questioned—expressed succinctly by individuals responding to a blog-post by the Director of the Nuffield Council on Bioethics reflecting on the importance of trust and transparency in the management of the crisis, who variously commented:

> "Notwithstanding the correctly much vaunted 'science' held as justifying not allowing loved-ones the chance to accompany the dying process, I have been concerned at

who has being formulating this kind of rule, using what process, and precisely what rights, interest, risks and benefits are being drawn into the analysis? Do we have a failure of moral proportionality?"[1] 1

"It's obvious why we don't want mass movement of people, but why we don't want a very elderly wife sitting with her very elderly husband as he dies in a care home is not so clear."[2] 2

The power and perils of networked digital technologies

In contrast to social policy instruments, such as physical lockdown orders, the power of networked digital technologies lies primarily in several important characteristics: their capacity to automate data collection in real-time and at scale; to automate decision-making; and their malleability, including their potential to be configured to operate with considerably less reliance on active citizen cooperation. If such technological tools could accurately track the movement of individuals across an entire population, they could considerably enhance the effectiveness of the government's response to the pandemic. Many countries have therefore sought to automate the collection of data about the movement of individuals and their physical interactions with others. Some have rolled out contact-tracing apps intended to generate automated alerts when two app-enabled devices come within a pre-specified proximity of each other and at least one of the device owners is identified as a suspected (or confirmed) virus carrier. Leaving aside serious doubts about whether these apps work effectively and as intended, networked digital tools—like their more conventional social counterparts—nevertheless impose burdens on citizens, albeit of an intangible form, often in the form of interferences with their rights to privacy. These rights are of such moral and political importance that they are widely recognised as human rights and thus have peremptory moral force which cannot be lightly overridden, unless a compelling necessity is demonstrated and the interference is proportionate to that need. Yet as Rob Kitchin observes in his contribution to this

volume, the prevailing attitude appears to be that 'using the tech, even if flawed or unsuitable, is better than not using it.'

Given the potential power, sophistication, and opacity of these systems, the apparent inattention to testing, validating, and attending to the consequences of error and other unintended effects of the digital tools proposed to tackle COVID-19, including their impact on human rights and important moral values, is seriously troubling. Because these systems can be configured to operate in ways that do not require active citizen cooperation, they entail important design choices about the extent to which their data-gathering and decision-making capacities provide citizens with the possibility to opt out. These choices also entail making trade-offs between conflicting values. For present purposes, this entails weighing the need and importance of obtaining up-to-date, accurate, and highly granular information across the population—and evaluating whether these systems will actually deliver the desired level of functionality and accuracy—against the extent to which such systems interfere with individual and collective privacy, while taking account of errors and their consequences for informational accuracy, their likely impact on the effectiveness of containment measures, and
3 the consequences for affected individuals.[3] In addition, because capturing data on each person's movements across time and space is highly sensitive, decisions must also be made about how that data may be used, who can access it, whether and how it will be stored, for how long, whether in identified, pseudonymised or anonymised form, and the stringency of its security. All these decisions will implicate human rights and moral values, including rights to individual and collective privacy, to data protection, to freedom of movement and other fundamental rights, and to equality and distributive justice. Furthermore, the opacity and ease with which these systems and datasets can be repurposed for multiple and unrelated ends raises the danger and prospect of mission creep. Many commentators, including civil society organisations, have thus expressed considerable anxiety that these technological systems might be used in ways that seriously threaten basic liberties and freedoms.

Accordingly, although networked digital technologies have invaluable and extensive capabilities that could seriously enhance the effectiveness of pandemic containment, their automaticity, speed, scale, and data-generating capabilities mean that their potential for abuse and overreach is vastly greater than the risks of abuse associated with more conventional social instruments of control, in the form of rules backed by penalties. Not only are conventional rules enforced on a case-by-case basis, but they do not suffer from the same level of opacity and cannot be so readily repurposed.

Democratic accountability, participation, and effective safeguards

The extraordinary power and potential of networked digital technologies highlights why transparency, public consultation, and robust and trustworthy systems of oversight are vital and indispensable, at least in democratic societies committed to respect for individual liberty and freedom. The need to establish and implement adequate oversight systems and safeguards is made more urgent if these technological systems are developed and implemented by private providers. Yet the urgency of the state's need to draw upon the technological capacities and expertise of commercial firms may result in the implementation of privately developed technological systems without adequate democratic oversight. This both significantly increases risks of exploitation and abuse, and makes it more likely that the systems themselves will prove impossible in practice to roll back, even after the pandemic has passed. Hence Naomi Klein's alarm at the colonising ambitions of the digital tech sector, which the pandemic has only accelerated.[4] 4
Although Klein recognises that networked digital technologies will have an important role in protecting public health moving forward, she warns that COVID-19 is enabling their rapid acceleration into the realm of critical services such as health and education without democratic participation and oversight, allowing Big Tech to eschew all responsibility for any resulting collateral damage.

Public trust, transparency, and accountability in governmental decision-making

The need for effective oversight and safeguards over the development and deployment of networked digital systems

aimed at tackling COVID-19 is merely an application of the more general need for transparency, openness, and accountability by governors to the citizens whom they are required to serve. Although the so-called 'state of exception' may justify a relaxation of limits that might otherwise apply to governmental power, it does not mean—at least in democratic states—that anything goes. Firstly, it does not alter the basic terms of the social contract by which citizens forgo some of their liberty and freedom in return for the state's obligation to provide them with basic security. Although the exceptional demands of the pandemic may justify loosening some procedural constraints that otherwise apply to the exercise of governmental authority, it does not dispense with them altogether. Secondly, and perhaps even more importantly, without sufficient transparency and accountability in the exercise of decision-making authority, those in government will not sustain the trust, cooperation, and solidarity of citizens, upon which effective interventions to contain the virus ultimately depend.

References

1. See comment by Nicola Stingelin: https://www.nuffieldbioethics.org/blog/covid-transparency-and-trust

2. See comment by Julian Hughes: https://www.nuffieldbioethics.org/blog/covid-transparency-and-trust

3. For example, in digitised contact tracing systems, this includes both false positives, i.e. those who erroneously receive an alert that they have been in contact with a person who has contracted the virus, and false negatives, i.e. those who have been in contact with a person who has contracted the virus but the system has failed to register this interaction and hence the potentially infected individual does not receive an alert.

4. See: https://www.theguardian.com/news/2020/may/13/naomi-klein-how-big-tech-plans-to-profit-from-coronavirus-pandemic

Karen Yeung is Interdisciplinary Professorial Fellow in Law, Ethics and Informatics at Birmingham Law School and School of Computer Science at the University of Birmingham.

WHO COUNTS?

CONTACT TRACING

AND THE PERILS OF PRIVACY

Os Keyes

Exceptional times demand exceptional measures, and are correspondingly frequently enabling for policymakers, proposals, and organisations that chafe against the conventions and regulations of regular life (see the chapter by Cruz-Santiago). In the current COVID-19 outbreak, a prominent example is the advocacy of technological solutions to the issue of contact tracing: that is, tracking people who have associated with an infected person, and so may be infected in turn. Whereas contact tracing was historically undertaken through human labour—volunteers or public health workers contacting the (self-reported) associates of an infected person—this current crisis features a vast array of proposals to integrate automation and technological surveillance.

In the country-based case studies featured in this book, we see proposal after proposal for technological solutions to

contact tracing—most commonly based around a smartphone app (see the chapters by Álvarez Ugarte and Musiani). Generally speaking, the proposal is for citizens to load an app onto their phone that regularly pings nearby devices using Bluetooth. As they pass through the world, a person generates a datalogical trace and map of all those people they have been proximate to—people who can be contacted *using* that data should the original user test positive.

Concerns about these proposals are frequently oriented around the potential for privacy violations; traces of a person's travels, friends, and associates are inherently sensitive, and their security depends heavily on the way in which they are collected and stored. As a result, it has been unsurprising to see academic scholarship, media work, and public opinion focus largely on the question of privacy in evaluating the design of these apps. These concerns are important, but their prioritisation has obscured more fundamental questions about an app-based approach. Who can use these technologies? How does that change whose lives and illnesses matter? And: is privacy always a good thing?

Although often treated as a universal—and universally accessible—moral good, privacy is actually neither of those things. Instead, it is frequently highly contextual, as is its desirability. Consider public services: if a person wishes to access income support or medical systems, the presentation of a state identity card, tax records, or pay slips is often a requirement. Now, requiring this data—and centrally logging it—is certainly inhibiting to the privacy of the person in question. But it would be ridiculous to argue that undocumented immigrants or homeless people, lacking access to this data, and thus lacking access to services many people need to live, are in fact *benefiting* because their privacy remains intact. A better view requires attending to what Gilman and Green refer to as 'the surveillance gap': the ways in which society's most vulnerable members' 'functional [invisibility]' to surveillance systems can cost them dearly when such systems govern access to resources.[1]

1

In the case of contact tracing, the focus on the privacy of data collected through smartphone apps obscures who is left

out of data collection entirely, and what the consequences are of that. Rob Kitchin's summary of the situation in Ireland is one of the few pieces to note the high number of people (in Ireland's case, 28% of the population) who do not have a smartphone. From a contact tracing perspective, they have privacy—but that privacy heightens their vulnerability to becoming infected, through reducing their chances of being notified in the event they were exposed to an already-infected individual.

Further, those left out of these medical surveillance networks are not randomly selected: the absence of a smartphone often corresponds with age and income, with the poor and very old least likely to have the resources and inclination to possess one—while also being the most likely to suffer as a result of the pandemic. In nations without robust social security systems, it is the poorest among us who can least afford to take time off from work, and who have the least access to medical care. In highly racialised nations, as Whitney Laster Pirtle notes in her case study of the United States, this poverty and vulnerability is additionally racialised in its distribution.[2] Similar concerns are raised in the chapter by Julie E. Cohen with regards to other aspects of normative adaptations to the outbreak—in particular, the viability of self-isolation for people in environments where physical space is not a resource that can be taken for granted.

2

Talking about privacy in understanding these technologies is necessary. But giving privacy primacy risks giving the game away: implicitly accepting that a technological solution is the correct one, and arguing over data storage models as the site of concern. Instead, my point here is that any high-technology solution implicitly establishes preconditions for use—preconditions many people are unlikely to be able to meet. And when the state response to the crisis treats that solution as the only game in town, the consequence is not privacy but vulnerability.

Activist-scholars should absolutely be pushing back against centralised data collection and the use of the current crisis as an excuse to legitimise new modes of surveillance. But such work needs to foreground the existing inequality of the

world and societies we are living in, and understand that just as access to healthcare, food, and housing is fundamentally uneven, so too are the consequences of surveillance. By extension, justice-oriented solutions to contact tracing need to not only protect privacy but—recognising the trade-offs inherent to any surveillance technology, however well-intentioned—also to ask who is left out of the current proposals altogether and how to enable their access in the short term, while addressing the structural inequalities that caused this unwilling invisibility in the longer term.

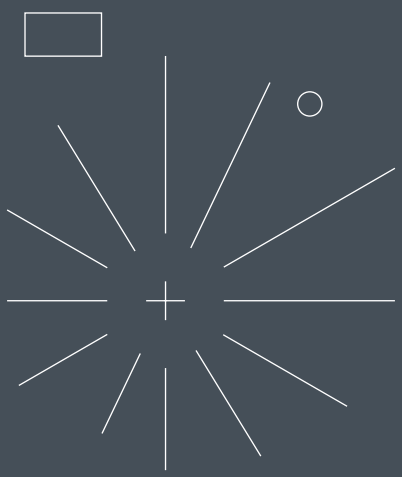
References

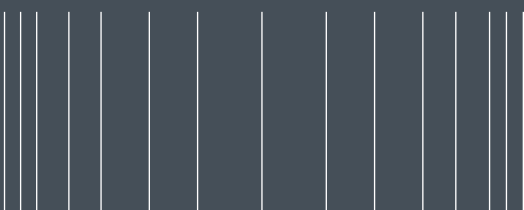
1. Gilman, M. & Green, R. (2018) The surveillance gap: The harms of extreme privacy and data marginalization. *NYU Rev. L. & Soc. Change.* 42: 253.

2. Laster Pirtle, W. N. (2020) Racial capitalism: A fundamental cause of novel coronavirus (COVID-19) pandemic inequities in the United States. *Health Education & Behavior:* 1090198120922942.

Os Keyes is a PhD candidate at the University of Washington in Seattle, United States. They are supported by a Microsoft Ada Lovelace Fellowship.

THE DANGERS OF DIGITAL CONTACT TRACING:





LESSONS FROM THE HIV PANDEMIC

Dragana Kaurin

The COVID-19 pandemic is the first in which digital contact tracing has been deployed widely—including in India, China, South Korea, France, Germany, and the US, where it has been heavily criticised by a number of civil society organisations. Many authors in the Country Dispatches section of this volume have expressed privacy concerns about smartphone-based contact-tracing solutions, the loss of agency and consent about one's own data, and its repurposing for surveillance.[1] It is therefore worth asking whether digital contact tracing would even work in the first place—considering that we are dealing with a virus that we are still struggling to understand and manage—and what the consequences are of relying too much on quantitative data analysis and technological solutions.

1

In a rush to provide all the relevant information about the new virus to the public, media sources have often provided conflicting information and advice from government institutions, epidemiologists, and public health organisations. In this era of hyperconnectivity, misinformation has spread widely and quickly, causing panic and stigma towards those who have

tested positive for the virus.[2] After urging people not to buy masks unless they were immunocompromised, in early April the US Centers for Disease Control and Prevention (CDC) changed their guidelines and recommended that everyone wear cloth face masks in public, causing more confusion and distrust.[3] With new information coming out constantly, it is still difficult to tell how many people have been exposed to the virus without exhibiting any symptoms, or why others with no pre-existing conditions have died from it.[4]

As of June 2020, we also don't know whether those who have had COVID-19 are now immune to it, or if they could become sick again if re-exposed.[5] Neither is it clear how reliable the available COVID-19 antigen tests are, or the antibody tests that indicate a prior infection.[6] Before it was given a name, one of the earliest articles about COVID-19 published in Hong Kong's East China Morning Post referred to it as a 'mysterious pneumonia' and quoted a local public health expert as advising: 'There's no need to panic. First, compared with 2003, we have better systems in notification, testing and infection control. We also have medicines that we can try.'[7]

The article has obviously not aged well, with over 11 million cases and 530,000 deaths globally six months since publication, as many other articles about the pandemic being published now will similarly not age well when we are predicting the unknown. It reminds one of the now-famous 1981 New York Times article titled 'Rare Cancer Seen in 41 Homosexuals' describing the first suspected cases of AIDS in the US.[8] In a similar, panicked tone, the article tries hard to connect all the seemingly disparate pieces of information, and sadly misleads the readers just as the South China Morning Post article did almost 40 years later: 'The medical investigators say indirect evidence actually points away from contagion as a cause [because] no cases have been reported to date outside the homosexual community or in women.'

Since the first AIDS cases were reported in the US in June 1981, or Gay-Related Immune Disorder (GRID) as it was known then, sociologists at institutions like the CDC took on the initial task of interviewing patients for contact tracing,

and documenting the environmental and lifestyle factors that would help the CDC later deduce that the immunodeficiency is caused by a virus and not chemicals from cleaning products, or recreational drug use, as initially thought.[9] To be able to get this data, a great amount of trust had to be established between the sociologists running the interviews and the patients—who were facing a lack of treatment options, a lack of protection from stigma and threat of physical violence, as well as the legal repercussions of living as gay men in the US during this period.

9

> "To investigate the possibility that AIDS patients could be linked sexually, [Bill] Darrow was dispatched to Los Angeles... 'I felt confident,' he recalled, 'that I could talk to the people who were infected, make them feel comfortable, not embarrass them, assure them that I would not violate their trust, and assure them that although I was not a medical doctor and couldn't help them at all, that whatever I learned I would try to see to it [that] it would be beneficial for them and other people that they were concerned about.'
>
> At a time when declarations of homosexual activity could lead to felony charges in several states, the CDC investigators were well aware of many possible reasons for noncooperation... Through their interviewing efforts in March and April 1982, Auerbach and Darrow were able to establish sexual links between nine out of thirteen of the twenty-six earliest reported KS/OI cases in southern California."[10]

10

Without this important qualitative data, it is difficult to imagine how long it might have taken the public health community to make the same deductions about what caused the immune deficiency seen in patients in the early 1980s, and make the connection to haemophilia, intravenous drug use, and blood transfusions. It would have been nearly impossible to trace how the virus had already spread in Europe, Haiti, and Central

Africa, where people had already been dying of the disease for decades by that point.

It is clear from the Country Dispatches in this volume that contact tracing for COVID-19 requires the trust and participation of the community, large-scale testing, and robust qualitative data to help investigators understand exactly how a virus is spread between contacts, and the risk factors that make some more susceptible than others. This is made more difficult by digital contact-tracing apps with compulsory location tracking like those used in China. Even apps that use Bluetooth instead of GPS, which are designed to be less intrusive with data collection, do not provide reliable and sufficient quantitative data regarding proximity and signal strength.[11]

11

Without gaining the trust of patients and without practicing consensual data sharing, we will potentially face the heavy consequences of relying too much on technology to save us—and therefore missing out on the qualitative data gathering by social researchers that has traditionally formed part of the early response in managing a novel virus pandemic. At a time when there is very little trust in leadership and the administration—as seen in the US currently—people seem to be concerned about how their data will be handled, and are questioning why Apple and Google are providing the contact-tracing service instead of the government.

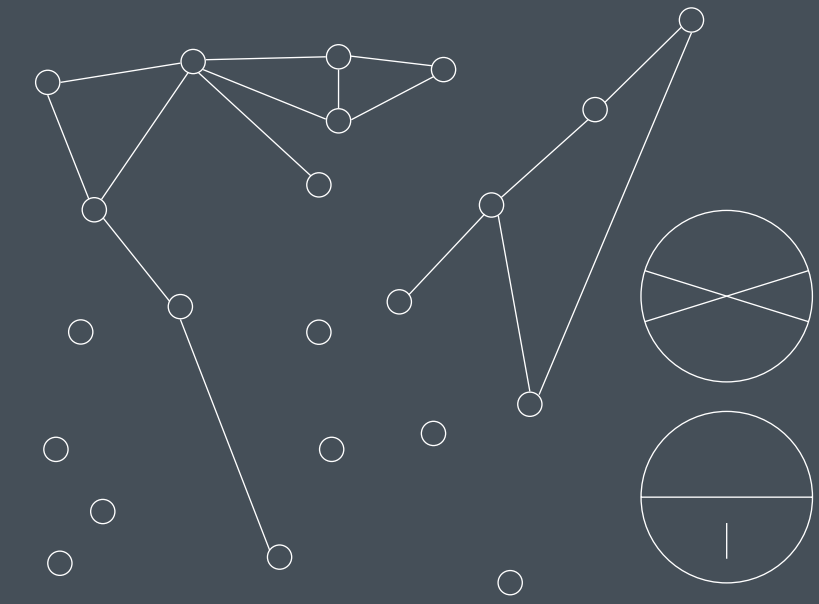
As a result, there have been no successful deployments of contact-tracing apps in the US so far. South Dakota has seen the most success—though only two percent of residents volunteered to share their data. This speaks volumes about how little trust there is in local and federal institutions; and it is quite unlikely that they will regain the trust of the public by outsourcing public health matters to the private sector, even if they are better equipped to provide the service.

References

1. See: https://www.nytimes.com/2020/03/01/business/china-coronavirus-surveillance.html
2. See: https://www.technologyreview.com/2020/02/12/844851/the-coronavirus-is-the-first-true-social-media-infodemic
3. See: https://www.yalemedicine.org/stories/wear-covid-mask
4. See: https://www.denverpost.com/2020/05/11/coronavirus-covid-what-we-know-now
5. See: https://www.newyorker.com/science/medical-dispatch/what-we-dont-know-about-covid-19
6. See: https://www.propublica.org/article/coronavirus-tests-are-being-fast-tracked-by-the-fda-but-its-unclear-how-accurate-they-are
7. See: https://www.scmp.com/news/china/politics/article/3044050/mystery-illness-hits-chinas-wuhan-city-nearly-30-hospitalised
8. See: https://www.nytimes.com/1981/07/03/us/rare-cancer-seen-in-41-homosexuals.html
9. Shilts, R. (1988) *And The Band Played on Politics, People, and the AIDS Epidemic.* New York: St. Martin's Press, p. 87.
10. McKay, R. A. (2017) *Patient Zero and the Making of the AIDS Epidemic.* University of Chicago Press, pp. 104-106.
11. See: https://theintercept.com/2020/05/05/coronavirus-bluetooth-contact-tracing

Dragana Kaurin is a research fellow at the Berkman Klein Center for Internet & Society at Harvard University and the founder of The Localization Lab.

REINING IN HUMANITARIAN



TECHNOLOGY

TECHNOLOGY

Anonymous I

Smart people work at international NGOs. Maybe you know some of them. You know they agree with you about the importance of responsible data, the great risks of harm they involve. But what on earth are they *doing* in there?

It is late January.

The BBC News podcasts that soundtrack my commute bring me the first reports of COVID-19 as they emerge. Rationally, I know this could be serious, but the grind of work and home keeps urgency at bay.

At the office, our customary internal chaos is all-consuming. I have been working for almost a year to institutionalise a basic responsible data policy for our data work, which is core to our mission, but the process has stalled and the report I have been writing languishes in an open tab. The work is high priority, but I am the only staff member assigned to it and run several other programmes. Frankly, it is more important that we be seen to be doing this type of work than that we get it right. Responsible data is part of my background, and I feel like I am failing. Embarrassed, I am avoiding my usual list-serves and colleagues. I file new

reports and guidelines on data ethics for later reading in some mythical free time-slot. Our programmes seem stuck in contract negotiation, so I tell myself there is time and I will get to it. Next month will be better.

It is mid-February.

The BBC now spends half of every podcast on COVID-19. My colleagues and I exchange worried updates in the corridors. We begin to realise how serious this will be. I quietly up our home preparedness game. Diapers, bottled water, and back-up bags of coffee huddle next to the Christmas decorations and abandoned strollers in our storage space.

I lurk in responsible data chats and email threads as irate colleagues exchange news of invasive and ineffective contact-tracing apps. Tabs multiply in my browser. I have been in this field for more than a decade, I know the drill. The ideas will be exciting, the promises grandiose. The risks will be enormous, the payoff dubious. Many of these ideas will get investment. Some may even get built. Most will not be impactful enough to cause a problem. All will be a waste of time and money. A few will cause harm, and in all probability, no one will ever know.

It is late February.

We discuss how to take our in-person team remote. A friend is pretty sure they have had COVID-19 and recovered. We start cancelling international travel and grapple with what this means for our work plans and budgets. The office empties out.

I realise slowly how much of this response will reach for data as the solution, and how underprepared my employer is for it. There will be a free-for-all, and it will be partly my fault. I apologetically resuscitate old email threads with partners and colleagues, asking for meetings to take forward development of our responsible data policy. Colleagues are happy to help, but overstretched. Governments are asking them to pivot their programmes toward the COVID-19 response.
It is early March.

I visit my family, and wonder when I will be able to see them again. I feel relieved I have stocked up, and I am very aware of my privilege.

Our leadership ask us to outline how our work could be used in the COVID-19 response. I review the document and leave comments in a red font. Some of the worst ideas are taken out, but I still feel sick and guilty reading it. We have no responsible data policy. While many of us understand the concepts, there are no systems to enforce ethical behaviour, so people can be forgiven for constructing interventions that do not meet responsible data guidelines. We have no guardrails.

We hold a meeting to discuss our policy and all agree that it is important. We figure out a way forward. Only a small piece of document review stands in the way of us piloting our new process for one of our programmes.

It is late March.

My partner and I are now at home, and so is our pre-schooler. I have even less time to work. I grapple with guilt continually—about parenting, about work, about being so tired that I fall asleep when I should be spending time with my partner. Our supplies are holding up. My introversion is not.

At a meeting, a donor colleague challenges the group to abide by the principles and frameworks they agreed to before the pandemic. By our standards, this is robust language. Privately, they share that they cannot stop other departments organising hackathons and internally circulating unsolicited private sector tech ideas. Under an unprecedented caseload, everyone needs to point to innovative, moonshot responses that might allow them to mount a meaningful response to COVID-19.

We are told to pivot as much of our work as possible to the COVID-19 response. It seems our donors expect it. We replan, adding COVID-19 elements to some projects, delaying or cancelling others, starting new things. In the upheaval, I never remind colleagues to comment on our draft responsible

data practices. We never set up the pilot of those practices that would have been the next step, even as our adjusted programmes gear up for accelerated implementation.

It is mid-April.

At home, childcare hand-offs are now wearily familiar. Days crawl, and weeks flash by.

At work, a month into lockdown, some activity has slowed. Pivoted programmes are either underway, in negotiation or abandoned. The impacts of the pandemic on the Global South have not yet become apparent. We feel like we are in a holding pattern. Our responsible data practices are as theoretical as ever. Those pivoted programmes, inching ahead, are still without guardrails.

But amidst the gloom and grind, some glimmers of hope. Specialist partners are providing blunt feedback, pointing out faulty assumptions and gaps in our analysis. Colleagues are receptive. I start a new email thread. If we review our draft practices now, they could be operational in one programme by the summer.

The programmes we support analyse massive amounts of data, belonging to hundreds of thousands of people. The analytics we provide could, in theory, influence government policy affecting millions more. In years to come, the systems we set up could be weaponised against vulnerable people. And the slim protection I am trying and, mostly, failing to put in place is that smart people ask themselves some questions before they start. It is a pretty flimsy constraint on a poorly understood, and depressingly clumsily directed, information superpower. Perhaps the most I can do is to try to ensure that we learn from our impact, whether intended or unintended.

Life in the trenches of an International Organisation or international NGO is inherently morally questionable at the best of times. We are so busy. Our impact feels so small. And on this issue, about which I care very much, I have done less

than nothing. I am complicit in things I would have railed at from the outside. But do you see, now, why that is?

The only way we will ever get better at this, is if somebody makes us.

DIGITAL EMERGENCY

IS/AS

THE DIGITAL (NEW) NORMAL

Angela Daly

'Se vogliamo che tutto rimanga com'è,
bisogna che tutto cambi' ('For everything
to stay the same, everything must change')
– *The Leopard* by Giuseppe Tomasi di Lampedusa

The COVID-19 pandemic has brought huge changes to humanity's way/s of life, with no country completely untouched by disruption. However, in this disruption, I see many themes which evidence continuity with pre-existing problems, inequalities, and (negative) tendencies in digitisation, ultimately contributing to a less just digital world. There are a few aspects of the COVID-19 response which demonstrate glimmers of hope for a better world, including a digital one, being possible. But my fear is that these will remain marginal and instead hegemonic power will be consolidated even more in the context of this state of emergency. I hope I am proved wrong.

The pandemic has disrupted my life to a great extent, both personally and professionally. I am an embodiment of the contradictions at the heart of the digital society. While I rail

against some aspects of digitisation and stubbornly resist them, I find myself increasingly willing to use my debit card to pay for even the smallest of purchases, and am meeting everyone—colleagues, students, loved ones, capoeira camaradas, my Gaelic teacher—via Zoom. I type this in a Google Doc. Part of this paradox has included my advocacy and activism on COVID-19 data gathering and surveillance at home in Scotland/Alba—I have been working closely with the main UK digital rights NGO Open Rights Group Scotland to demand more transparency about, and human rights protections for, the data the Scottish Government is collecting in its COVID-19 response while also advising the Scottish Government as a 'critical friend' on its COVID-19 Data Taskforce. How the politics of Brexit, devolution within the UK, and Irish reunification are playing out in the COVID-19 pandemic response deserves its own detailed study; but notable for our purposes is the fact the Scottish Government has not wholesale embraced the NHSX app being developed 'down south' and seems to be adopting a more privacy-friendly approach.

The NHSX app and the central UK government response to COVID-19 brings me to the first theme of everything changing yet everything staying the same—the role of private companies in technology provision and procurement for government COVID-19 responses. In the UK, NHSX has a track record of highly problematic collaborations with tech giants in the form of the (ultimately illegal) DeepMind partnership (see chapter by Mollichi et al.). When the pan-demic was looming at the UK's shores, the British government invited big tech representatives to 10 Downing Street almost two weeks before the country went into lockdown, and the day before the government ceased (manual) contact tracing. The UK might be a particularly egregious example but it is not alone. In other contributions to this volume, the role of tech giants in providing key aspects of countries' COVID-19 responses is prominent—from Amazon's role in Canada (see chapter by Wylie), to Palantir in Germany (see chapter by Wagner), to GAFAM powering the transition of Brazil's com-panies, universities and schools to online distance learning (see chapter by Evangelista & Firmino).

The second theme of change yet everything staying the same is the way in which COVID-19 and the tech response expose, intensify, and amplify pre-existing inequalities. These pre-existing inequalities include the precarious and dangerous position of low-paid, often racialised, workers, such as those in the gig economy in the US (see chapter by Cohen) or migrant workers in Singapore (see chapter by Chen & Poorthuis). The tech response to COVID-19 also highlights pre-existing digital divides such as in Jordan (see chapter by Sharbain & Anonymous) and Ireland (see chapter by Kitchin), made all the more acute by so much of life—including work, education, and maybe also exposure to disease—now being digitally mediated. Who is not counted in 'the data' is also significant—the epistemic injustice suffered by the Indigenous peoples of North America includes now the insufficient gathering and sharing of health information in the Navajo Nation, compounding the pandemic's impact there and impeding Indigenous data sovereignty (see chapter by Duarte).

The intensification of (often problematic) digitisation is the third theme of everything changing yet staying the same. Authoritarian governments throughout the world are seizing on the state of exception to consolidate power, amplifying their control, and in many cases are intensifying problematic data gathering and sharing, such as in Hungary (see chapter by Böröcz), the Western Balkans (see chapter by Kostić et al.), and Uganda (see chapter by Mwesigwa). As well as my own petty experience, the digitisation of money abounds elsewhere, as can be seen in Jordan (see chapter by Sharbain & Anonymous).

What then of the glimmers of hope for another, better (digital) world? A key objective of the *Good Data* book I co-edited in 2019 was imaging and implementing better data practices. There is little cheer from these global reports. The citizen-orientation of South Korea's private sector apps (see chapter by Kim & Yoon) and Japan's decentralised app (see chapter by Murakami Wood) do make a somewhat refreshing change from the centralised top-down approach of the UK (see chapter by Mollicchi et al.) and France (see chapter by Musiani). South Africa's very clear mechanism in the form

of a dedicated COVID-19 judge to uphold constitutional rights in, inter alia, oversight and limitations on data retention (see chapter by Gillwald et al.) is a model which should, in principle, be followed—or at the very least inspire—elsewhere. Concerns about US tech giants' control and influence over Australians' data seems to have motivated local procurement from companies such as Atlassian (see chapter by Johns). None of this is perfect and may still be far from our and others' notions of good data, data justice, and so on—but these examples do show that there are political economy choices in governments' tech responses to COVID-19 and that some choices are indeed better than others.

It is my hope that things do not remain the same during and after COVID-19, that we jettison the aspects of 'normality' which should not have been normal, and continue with the aspects of life under emergency which are indeed healthier—less carbon emissions for one. The continuation of movements for justice in these exceptional times, such as the protests in the US and solidarity movements elsewhere for Black lives in the wake of George Floyd's murder by police, which occur as I write this, demonstrate viscerally why change is needed and things—such as pre-existing inequalities—cannot just stay the same, or be allowed to worsen.

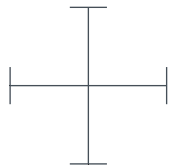
Will data be part of continuing the problem or part of the solution?

I hope for the latter, but I fear the former.

Angela Daly is senior lecturer (associate professor) in law and technology and co-director of the Strathclyde Centre for Internet Law & Policy in Glasgow, Scotland.


ARGENTINA
LAYERS OF CRISES:
WHEN PANDEMICS MEET
INSTITUTIONAL
AND

ECONOMIC



HAVOC

Ramiro Álvarez Ugarte

In Argentina, COVID-19 arrived late and gave the government a chance to prepare. It took that chance: for now, the contagion curve seems to be under control and after the enforcement of a country-wide lockdown, the health system seems to be coping well with the slow rise of cases. The situation is not, however, sustainable. The lockdown is battering an already heavily battered economy, and it is predictably and disproportionately affecting those who are worse off. Something will have to give. Entering the lockdown was easy, but it is increasingly difficult to see how and when we will get out.

In that context, the state has simply insisted on old practices regarding the use of technology for governance purposes. In this brief comment I highlight two features of the emergency. The first is related to the constitutional structure that was adopted to produce the state of emergency itself. The second is related to the role that technology has played until now in the crisis, and the role that it may play in the future. I will argue that both features are connected.

First, the government declared the emergency through a *Decreto de Necesidad y Urgencia* (DNU, or a Necessity and Urgency Decree),[1] a rather peculiar constitutional power which allows the president to issue statutory-level decrees in cases of emergency. To understand its significance, consider this: through a DNU the president can change statutes passed by Congress. The COVID-19 DNU restricted many rights immediately and in non-trivial degrees: international travel was halted, travel within the country was heavily restricted, education suspended, and citizens were allowed to leave their homes only to buy groceries, except those who work in a sector deemed 'essential'. Congress and courts have remained, until the time of writing in July 2020, largely closed. While abuse of power has remained within the usual levels, the fact that the main institutional accountability mechanisms are not properly working should give us pause.

This development, however, was to be expected. Everywhere, the rise of the administrative state in the early twentieth century increased the power of the executive and decreased the power of legislatures. The constitutional power of issuing DNUs, established in 1994, is just a constitutional reckoning of that fact.

This 'primacy of the executive' in Argentina is important for understanding how governments use technologies in the country: to advance executive goals and programmes, often with little to no congressional supervision. There is a bureaucratic inertia that sustains these processes. When, in 1968, a *de facto* government established the national identity card system, it built it upon previous registration efforts under the direction of the burgeoning executive department. Similarly, when in the early 2000s, the national identity database was digitised it was—again—because of an executive decision exercising broad police powers. Biometric technologies in airports and open-source intelligence (OSINT) surveillance over social networks were also measures adopted by executive fiat. In the city of Buenos Aires, even though the CCTV system was established by law, it was the executive that controlled its expansion. The executive decided to add facial recognition last year that led to hundreds of people being confused with others.

The response to the COVID-19 crisis reveals the same pattern: executive departments across the country were the first adopters of tracking technology, although the process seems to be at an early stage. For instance, the federal government launched the CuidAr app which is mandatory for those who return from abroad. Public officials have suggested that it might be used in the process of a 'smart' lockdown relaxation.[2] Its purpose is for users to self-diagnose: the app will inform you whether you have COVID-19 compatible symptoms or not, based on the information fed into it. It also allows you to get a digital passport to move around, with a QR code that can be scanned at checkpoints (although a low-tech PDF form works as well). Several provinces have embraced a private initiative called CoTrack, which adds a geo-tracking tool to the self-diagnosis layer, which has yet to become fully operational.[3] The app promises to use one's location data (gathered through the phone's GPS) and Bluetooth to let you know if you have encountered someone who is infected. For now, the map does not show any useful information: it just states that it is in the process of gathering the data.

The problems these technological solutions pose are similar, and relate to the inadequacy of the oversight mechanisms that could prevent abuses and that would keep measures narrowly tailored to address the need at hand and bring transparency and openness to the whole process. For instance, Argentina's Data Protection Law is old and a bill that sought to bring it closer to the European GDPR standards is pending in the dormant Congress. The authority in charge of implementing the law lacks adequate resources to do the job (a historical problem)[4] and has so far failed to issue any statement or guidelines regarding tracking technology.[5] If the past is any indication, a COVID-19 digital passport as a measure to partially lift the lockdown should be around the corner. We sort of know what safeguards are to be demanded from these technologies.[6] But in Argentina two big questions await us.

First, what kind of social and political coalition will be able to demand that privacy-protecting measures are embedded in whichever tracking system is eventually adopted? This has always been a challenge, since only a handful of politicians have shown concern in the past about privacy

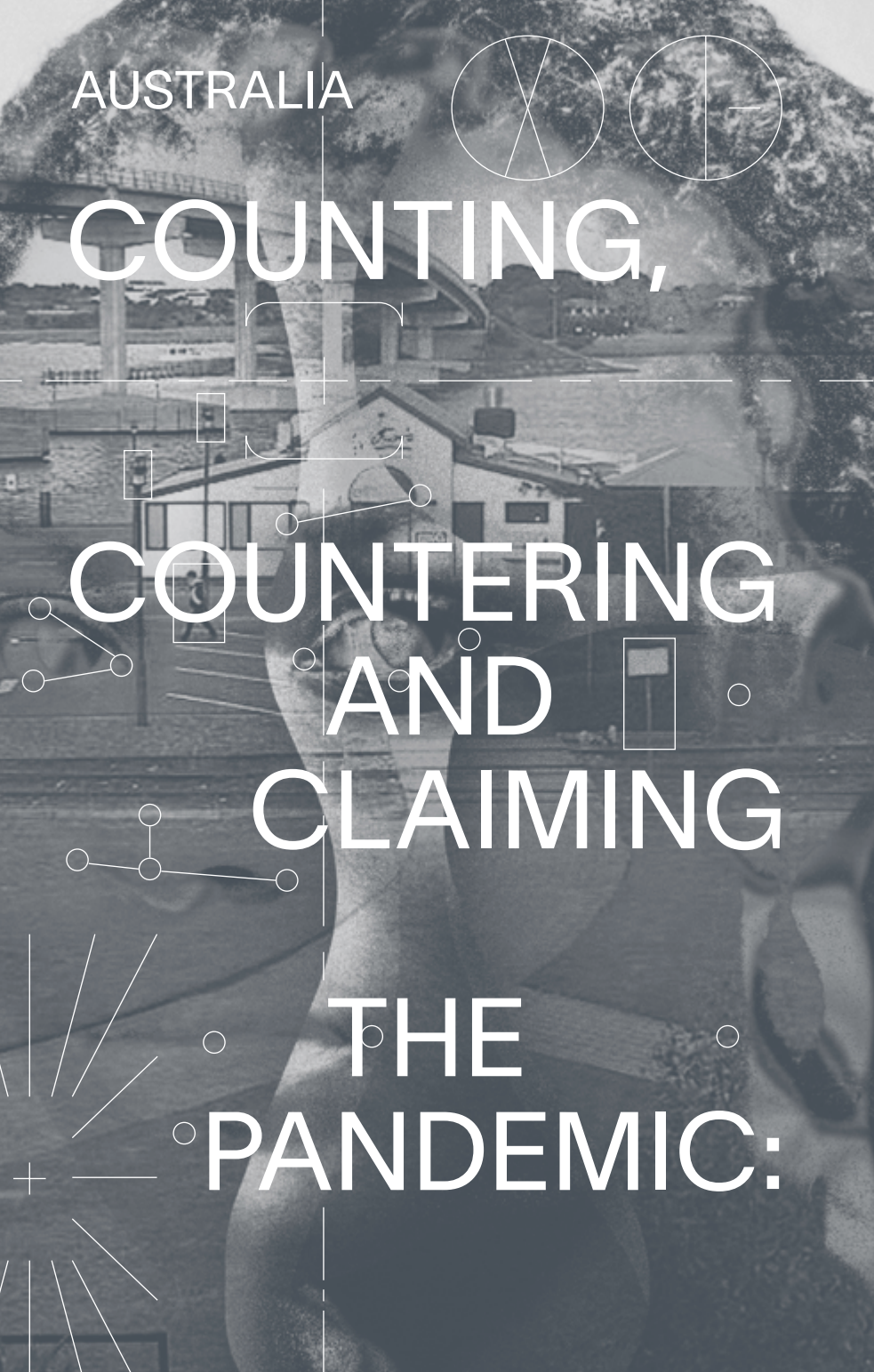
issues. Furthermore, it does not seem to be a priority in this context. Until now, oversight mechanisms have always worked deficiently.

The second question refers to the social support a pro-privacy political movement would need to succeed. To put it differently, will citizens care? I am very sceptical about privacy becoming a public demand that the political process would channel. Argentinians are used to paternalistic state policies under dictatorship and democracy alike. It would take too long to list all the measures that would have caused at least some stir in other countries and which were adopted in Argentina, as a matter of course.[7] Life-threatening viruses provide an especially good occasion for paternalistic states and societies to show their full potential. Why would privacy concerns become important in this time of need? This is the challenge the Argentinean privacy movement will have to address, sooner or later.

References

1. See: https://www.boletinoficial.gob.ar/suplementos/2020031201NS.pdf
2. See: https://www.argentina.gob.ar/aplicaciones/coronavirus
3. See: https://cotrack.social
4. See: https://ifex.org/images/argentina/2013/05/29/adc_derecho_debil_acceso_info.pdf
5. See: https://www.argentina.gob.ar/aaip
6. See: https://policyoptions.irpp.org/magazines/april-2020/contact-tracing-must-not-compound-historical-discrimination/ and https://www.eff.org/es/taxonomy/term/11560
7. See: https://vimeo.com/77142306

Ramiro Álvarez-Ugarte is a professor of constitutional law at the University of Buenos Aires, Argentina. He is a JSD candidate at Columbia Law School.



AUSTRALIA

COUNTING, COUNTERING AND CLAIMING THE PANDEMIC:

DIGITAL PRACTICES, PLAYERS, POLICIES

Fleur Johns

The following is a brief summary of some of the most significant expressions, in Australia, of the changing relationships between technology and authority manifesting in connection with the COVID-19 pandemic. It surveys some emergent governmental practices, key players, and major policy changes concerned with the pandemic and considers who may be gaining or losing from these developments.

Practices: growing government recourse to digital technology to mediate relations with constituents

At the end of March 2020, the Australian Federal Government launched an iOS- and Android-compatible mobile phone app (the 'Info App') and accompanying WhatsApp messaging service, to deliver data and guidance relating to COVID-19 to anyone downloading the app or subscribing to the WhatsApp channel. The Info App publishes daily updates on the national-level caseload, i.e., the cumulative number of confirmed cases, broken down by state and territory, and number of new cases since the preceding day. It also features a symptom checker, advice regarding government programmes and payments to address the

economic and social impacts of COVID-19, links to relevant public statements made by the Prime Minister or by the responsible committee and officials within the Department of Health, and links to COVID-19 information for each of the states and territories. In addition, the Info App provides an option for people to 'register isolation'—that is, those who are self-isolating may volunteer personal information for the stated purpose of 'help[ing] Commonwealth, state and territory governments to put in place appropriate steps' to '[s]afeguard public health and safety' and 'conduct appropriate analysis and research', and to contact the people so registered if necessary. An 'advice in your language' section directs users to a Department of Home Affairs website offering access to COVID-19-related government advice and information in 63 languages other than English, as well as to additional resources made available by SBS, the national public television, radio and online broadcasting network dedicated to multilingual broadcasting. Subscribers to the Australian Government's WhatsApp channel can obtain information and links of these kinds, and travel advice. Subscribers are also invited to share a link to the WhatsApp channel, to protect themselves, their family, friends and community.

In late April 2020, the Australian Federal Government launched an automated, mobile contact-tracing application (the 'Tracing App').[1] This was reported to be similar to, and possibly based on source code from, the Singapore TraceTogether app.[2] The Tracing App works by using Bluetooth to register any other app-loaded mobile phone with which an app-loaded phone comes into proximity (1.5 metres or closer) for at least 15 minutes.[3] The two phones in question will, via the apps, exchange anonymised IDs, which will then be stored encrypted on both phones for a period of 21 days, after which they will be deleted. Downloading of the app is voluntary, but promoted by the Federal Government with a view to reaching a stated target of 40% of the nation's mobile-phone-subscriber population. This goal is significantly higher than the take-up of the comparable app in

Singapore, where around 20% of subscribers have reportedly opted in. As of mid-June 2020, the Australian Tracing App had been downloaded more than 6.2 million times, meaning that a significant proportion of mobile phone subscribers (albeit not quite 40%) acceded to the government's pleas.[4]

The stated purpose of the Tracing App is to support the manual contact tracing currently being carried out by state and territory government health departments whenever someone receives a positive test result indicating COVID-19 infection (manual contact tracing having long been within public health departments' repertoire of responses to infectious disease).[5] When a person who has downloaded the app has tested positive for COVID-19, the state health department in their state of residence will receive notice of an app-holder having tested positive. They will then seek the infected user's consent to download the prior 14 days of the relevant mobile phone's contact data from a centralised national data store held on an Amazon Web Services server located in Australia.[6] The department may alert other subscribers that have downloaded the Tracing App with whom the infected user has come into contact, either via the app itself, or via corresponding mobile phone numbers. The Federal Minister for Government Services has publicly undertaken to eliminate the national data store, and advised that users delete the Tracing App, once the pandemic is over.[7]

Notwithstanding the centrality of the Tracing App to the Federal Government's public messaging—initially, widespread downloading was said to be a crucial precondition to the relaxation of social distancing requirements—it appears that its use for tracing may have been fairly limited to date and it may not, in fact, have been key to Australia's success in containing the novel coronavirus.[8] This is attributable, in part, to technical difficulties plaguing the Tracing App's operation and precision, especially on iPhones (which account for around half of all smart phones used in Australia).[9] This reflects a tendency discernible in other settings: to focus public attention and resources on the development of shiny new governmental technologies, with many of these not delivering on their rather hyperbolic promise, such that their actual deployment often comes

to rest on pre-existing, analogue work practices and workforces—many of the latter, in relative terms, both under-resourced and under-scrutinised.

Players: key beneficiaries of these changes

Facebook is clearly a major winner from the Australian Federal Government choosing to adopt its products and services as part of its efforts to communicate with the public surrounding COVID-19. The delivery of official government information and advice about access to government funding via the Facebook-owned WhatsApp—together with government promotion of this channel—encourage mobile subscribers to download and use WhatsApp. This government endorsement also helps to generate a public impression of WhatsApp and Facebook as safe to use, and as likely sources of reliable, even essential, information. The positive impact of this association is likely compounded by the fact that Australia's experience of COVID-19 was, as of the time of writing, far less devastating than other nations' in terms of death toll and hospitalisations, with the nation having achieved a comparatively rapid flattening of the curve in terms of rates of new infection, and relatively high per capita rates of testing.

The NASDAQ-listed, Sydney-headquartered, software development company Atlassian is another indirect beneficiary. According to media reports, Atlassian worked with Facebook to develop the government's WhatsApp channel described above.[10] One of Atlassian's Australian co-founders / co-CEOs confirmed, via Twitter, that the company will not be remunerated for any of its work for the government on COVID-19 matters.[11] Nonetheless, any positive media coverage of the app, and of Atlassian's pro bono contribution, will yield reputational gains for the company. Atlassian also, of course, took on some risk of reputational harm if things were not well-perceived publicly, although this does not seem to have materialised.

The Info App was designed and built by a relatively small, privately owned, Canberra-based technology services company, Delv, that has, since its founding in 1999, been developing mobile applications for a range of government agencies, as well as local and international organisations.[12]

Design and development of the Tracing App was carried out by the Digital Transformation Agency, an agency of the federal government.[13] The government initially ruled out working with Apple and Google in this connection. More recently, however, the Digital Transformation Agency has indicated that it is now working with Apple and Google with a view to integrating their exposure notification API into the Tracing App, in order to address problems experienced in its interface with the iPhone operating system.[14] Apple and Google seem, therefore, likely to emerge as winners too, by their gaining an opportunity to reinforce public perceptions of their indispensability to all aspects of contemporary life.

Some healthcare sector service technology providers may benefit from growing recourse to digital healthcare technology in connection with the pandemic. In particular, providers of diagnostic imaging services employing digital technology may benefit financially if higher-than-usual levels of CT scanning become apparent in connection with new diagnostic and therapeutic protocols adopted across the public hospital system (although reported decline in routine medical consultations in connection with the pandemic may render these outcomes equivocal). Expanded government funding for telehealth consultations may also encourage greater use of proprietary digital telehealth platforms.

Policy, policing, parliaments, and polling

The governing privacy policy for the Info App, described above, is the privacy policy adopted by the federal Department of Health (most recently in 2017)[15] under the Privacy Act 1988 (Cth).[16] Data use in connection with the Tracing App is also governed by a dedicated COVIDSafe App privacy policy.[17] In addition, amendments to the Privacy Act were enacted in mid-May 2020 to create offences for using data collected by the Tracing App for purposes other than contact tracing.[18] The government solicited a privacy impact assessment of the Tracing App from a private law firm, Maddocks. This assessment was made publicly available, as was the source code for the Tracing App.[19] Government policy-making in connection with COVID-19 has primarily proceeded by issuance of regulations and determinations under the Biosecurity Act 2015 (Cth),[20]

pursuant to the declaration of a 'human biosecurity emergency' at the federal level, and corresponding public health legislation and declarations at the state and territory level. Some of these regulations have created new police powers to enforce social distancing and other requirements. Police in at least one Australian state have announced plans to deploy drones to assist in their implementation.[21]

21

Parliamentary processes and potentially electoral processes are being subject to new routes and forms of digital intermediation in connection with the pandemic. The Commonwealth Parliament was adjourned in early April after the introduction of social distancing requirements, with the next in-person sitting scheduled for August 11, 2020. Parliamentary procedural rules (standing orders) were hurriedly amended in late March to permit parliamentarians to meet electronically rather than in person. That is reportedly how the so-called National Cabinet meets—a newly created body assembled to coordinate governments' decision-making in the pandemic that comprises the nation's prime minister and the premier or head of government of each of the states and territories. Work-related use of some digital video-conferencing services that are seeing exponential growth worldwide—specifically Zoom—has reportedly been barred for parliamentarians and public service employees at the federal level on the advice of the Department of Defence.[22] Instead, the federal government apparently preferred Microsoft software (including Microsoft Teams). A number of sub-national elections have been deferred and independent electoral commissions in each state and territory will be responsible for determining when and how they proceed. It is noteworthy, however, that Australia, where voting is compulsory, already has high levels of convenience voting by mail, so an all-mail election is the most likely alternative to in-person polling, rather than any other technologically mediated form of ballot. Digitally mediated political engagement outside state institutions has also been affected by the COVID-19 pandemic. Organisers of Black Lives Matter protests in Australia, working primarily through social media to rally attendance, have been fined for breaching public health orders.[23]

22

23

Finally, a Senate committee charged with conducting an inquiry into the Australian Government's response to the COVID-19 pandemic, including digital technology used in that response, is due to report on or before 30 June 2022.[24] 24

References

1. See: https://www.health.gov.au/resources/apps-and-tools/covidsafe-app
2. See: https://tracetogether.zendesk.com/hc/en-sg/articles/360043543473-How-does-TraceTogether-work-
3. See: https://www.itnews.com.au/news/govt-to-release-source-code-of-forthcoming-covid-trace-app-546884
4. See: https://www.abc.net.au/news/science/2020-06-11/coronavirus-contact-tracing-app-covid-safe-no-close-contacts/12343138
5. See: https://covidsafe.gov.au/help-topics.html
6. See: https://www.theguardian.com/australia-news/2020/may/15/covid-safe-app-australia-how-download-does-it-work-australian-government-covidsafe-covid19-tracking-downloads
7. See: https://www.itnews.com.au/news/govt-to-release-source-code-of-forthcoming-covid-trace-app-546884
8. See: https://www.theguardian.com/world/2020/may/24/how-did-the-covidsafe-app-go-from-being-vital-to-almost-irrelevant and https://www.abc.net.au/news/science/2020-06-11/coronavirus-contact-tracing-app-covid-safe-no-close-contacts/12343138
9. See: https://www.theguardian.com/world/2020/may/24/how-did-the-covidsafe-app-go-from-being-vital-to-almost-irrelevant and https://theintercept.com/2020/05/05/coronavirus-bluetooth-contact-tracing
10. See: https://www.itnews.com.au/news/australia-launches-covid-19-app-whatsapp-chat-539974
11. See: https://twitter.com/mcannonbrookes/status/1244117303018409985
12. See: https://itbrief.com.au/story/australian-govt-teams-up-with-delv-to-release-covid-19-app
13. See: https://www.itnews.com.au/news/australias-covid-tracing-app-better-than-singapores-health-chief-547126 and https://www.dta.gov.au/about-us

14. See: https://www.itnews.com.au/news/asd-vetting-code-on-australias-future-covid-trace-app-546800 ; https://www.theguardian.com/world/2020/may/06/covidsafe-app-is-not-working-properly-on-iphones-authorities-admit ; https://www.health.gov.au/resources/apps-and-tools/covidsafe-app/covidsafe-help

15. See: https://www.health.gov.au/using-our-websites/privacy

16. See: https://www.legislation.gov.au/Details/C2020C00025

17. See: https://www.health.gov.au/using-our-websites/privacy/privacy-policy-for-covidsafe-app

18. See: https://www.legislation.gov.au/Details/C2020A00044 and https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/bd/bd1920a/20bd098

19. See: https://www.health.gov.au/resources/publications/covidsafe-application-privacy-impact-assessment and https://www.dta.gov.au/news/dta-publicly-releases-covidsafe-application-source-code

20. See: https://www.legislation.gov.au/Details/C2020C00127

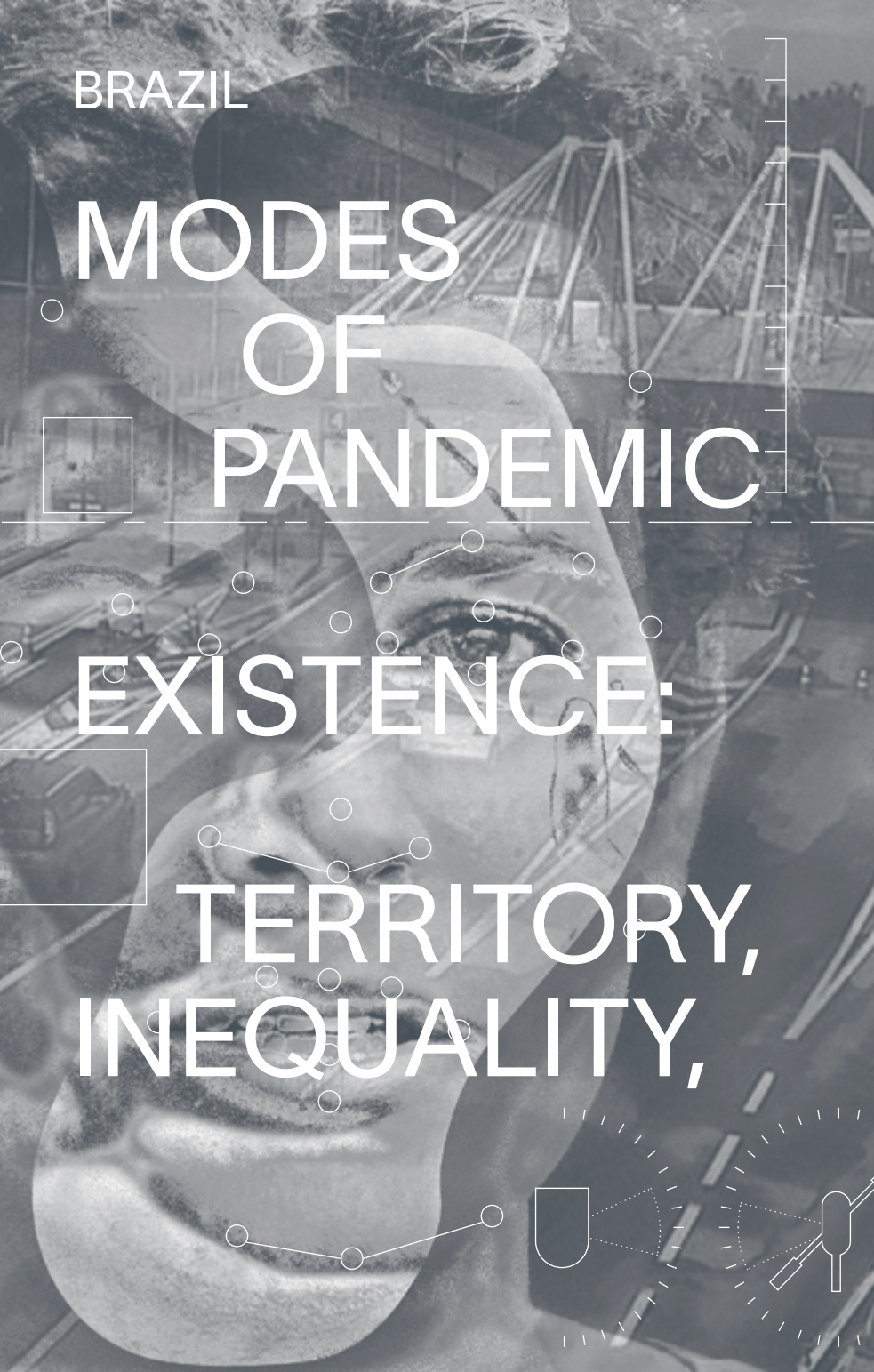
21. See: https://theconversation.com/pandemic-drones-useful-for-enforcing-social-distancing-or-for-creating-a-police-state-134667

22. See: https://www.channelnews.com.au/security-fears-see-govt-ban-zoom-use-by-pollies-agencies

23. See: https://www.abc.net.au/news/2020-06-06/melbourne-black-lives-matter-protest-organisers-fined-by-police/12329514 and https://www.smh.com.au/national/nsw/protesters-defy-ban-and-march-in-sydney-for-refugees-20200613-p5529x.html

24. See: https://www.aph.gov.au/Parliamentary_Business/Committees/Senate/COVID-19/COVID19

Fleur Johns is professor in the Faculty of Law at the University of New South Wales, Australia.

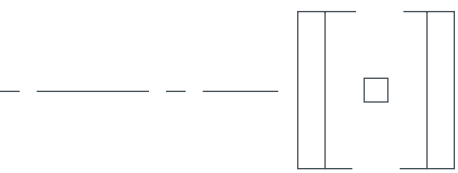


BRAZIL

MODES OF PANDEMIC EXISTENCE:

TERRITORY, INEQUALITY,

AND TECHNOLOGY TECHNOLOGY



Rafael Evangelista and Rodrigo Firmino

Brazil is well known for its history of social injustice and inequality, especially for the majority of its population of poor and extremely poor families.[1] Ordinary days pose enough challenges for those living with no access to formal jobs, governmental social programmes, quality education, sufficient healthcare, and with minimal conditions of sanitation (including regular water supply, sewerage, and appropriate garbage disposal and collection). The most recent—though already out of date—population census from 2010 recorded 11.5 million people living in high-density slums[2] in areas deprived of basic urban infrastructure and public services.

1

2

It must be said that the country is currently governed by people whose discourses fluctuate between the novel coronavirus being just a harmless flu[3] and it being a lab-designed disease devised by the Chinese government[4] as

3

4

a Communist plot for world domination. Although *prima facie* a healthcare issue, the COVID-19 pandemic can easily and
5 rapidly evolve into a humanitarian tragedy in Brazil.[5]

In contexts like this, government authorities and technology companies, but also ordinary citizens, become more open to fast solutions and uncritical experimentation with all kinds of technological fixes. Faith in science and technology increases, and everyone is thirsty for quick answers for either entirely resolving the crisis (e.g. a cure for COVID-19) or creating amenities that provide a sense of normality (e.g. home office solutions). It seems that we are at the crossroads of three disputed paths involving territory, inequality, and technology: the exception, the acceleration, and the rupture.

The exception is based on the belief that everything will be as it was once the virus is no longer a threat, and that normality is not just what we want to happen but in fact that this return will be materially possible. This is the view of the
6 president Jair Bolsonaro and most of his ministers,[6] who have been emphasising the lack of need for any urgency in policy. This is mainly based on conspiracy theories that the virus is either too weak to be concerned about, or that it is a powerful weapon against the Christian foundations of Western civilisation. In either case, when confronted with the devastating number of deaths, faith in quick fixes grows, and Bolsonaro is betting everything on the yet-unproven efficacy of hydroxychloroquine and chloroquine as permanent
7 cures[7] for COVID-19. His allies flood social media (especially WhatsApp groups) with daily waves of distorted articles on the alleged efficacy of this medication for tackling the pandemic. These include manipulated news of the supposed low efficacy of quarantine and social distancing measures. The strategy of spreading misinformation through social media is a powerful tool, used by Bolsonaro's supporters
8 during and following the 2018 general election.[8]

The acceleration of certain technological practices is also evident. A strategy of Silicon Valley-style companies around the world but also of China (although perhaps in another way or with other emphases), this path treats the current crisis as an opportunity to accelerate technology-driven

processes[9] that were already announced and slowly being implemented. Things like distance education serving the interests of surveillance capitalism, or remote work that deepens exploitation of working time and transfers fixed costs (rent, electricity, Internet, etc.) to the worker, are amongst the changes affecting the lives of many students and workers all over the world. In Brazil, for instance, companies, universities, and schools are rapidly signing up to technological solutions for studying and working from home, commonly adopting offers made by the biggest companies in this market (including Amazon, Apple, Facebook, Google, Microsoft, etc.).

9

The urgency of the current crisis enables an experimental setting for big technology companies. Such experimentation was previously restricted to exceptional places or subjects, such as the Global South, extreme poverty, or terrorism. However, with COVID-19 technology companies can argue for increased experimentation, in part, because a return to normality is virtually impossible without the use of technology. Technological fixes can be uncritically adopted to facilitate the new circumstances of everyday activities such as studying and working.

In Brazil, this is quickly happening in educational institutions and governmental bodies around the country. A mapping initiative organised by a consortium of research centres and public universities (UNESCO, University of Brasília, Institute EducaDigital, and Federal University of Pará) called Surveilled Education (*Educação Vigiada*),[10] has found that almost 65% of public educational institutions in Brazil have delegated their email servers to private companies like Google and Microsoft, and are therefore more easily exposed to the effects of surveillance capitalism. This data was collected before the pandemic, which means that the alienation of cybernetic infrastructures will deepen with increased, uncritical adoption of these technologies.

10

The idea of a rupture is underpinned by the hope that such a profound global crisis can be followed by a renewed critical take on the world socioeconomic order. The current crisis is the effect of an already unsustainable order. We could get out of it by creating other social structures—like unconditional

basic income, or a more broad public transit system—which are appropriate for the crisis but could become permanent, as they are likely to be more just, ecologically responsible, and lead to a more healthy life in general. State economic aid policies for informal workers and disadvantaged families are a strong message in that direction. Considered an unthinkable (i.e. too left-wing) measure until recently in Brazil, anything sounding remotely like a universal basic income was unlikely to be approved by the Congress, and yet, in the midst of
11 the COVID-19 pandemic, a similar temporary aid[11] was, in fact, proposed by the legislative branch (though not the president or the executive). There has also been an increase
12 in proposals for bills on raising taxation[12] of banks and the super wealthy; another move that would be otherwise improbable in periods of so-called normality.

In the slums and peripheries of large cities like Rio de Janeiro, many organisations and institutions are creating better ways and tools to help each other, and to increase empowerment of the populations living in these areas. Corona na Baixada
13 (#CoronaNaBaixada)[13] is an initiative that unites about 100 organisations from 13 cities in the region known as Fluminense Lowland, in the State of Rio de Janeiro. These institutions have a history of tackling inequality in poor areas of Brazil, and saw the seriousness of the COVID-19 crisis as a need to better articulate their actions on three fronts: (1) sharing experiences of local solidarity; (2) disseminating strategies to guide residents to stay at home; and (3) liaising with media outlets and public authorities in order to make visible the problems faced by these territories, and to monitor the measures that are being adopted.

These organisations—with a past in political activism against social injustice—seem to be better prepared and equipped to effect long-term political change both during and after the crisis. Focused on organic agriculture, the Landless Workers Movement (*Movimento dos Trabalhadores Sem Terra, MST*) has been donating food, milk, and prepared meals to informal workers and the homeless throughout the
14 country.[14] In several states, MST donated hundreds of tonnes of raw food in a period of three months (March, April and May 2020) after the pandemic's outbreak. They have also

been producing face masks and 70% alcohol, by converting a facility previously dedicated to artisanal *cachaças* (the famous Brazilian spirit made from sugar cane). The network of cooperatives connected by the movement has been instrumental in mobilising action.

Everything is moving very fast, and the idea that this is all just a temporary moment of exception seems less tenable every day. The resulting order (or orders?) that follow the crisis will depend on what is negotiated and imposed by the actors who are linked to the three scenarios outlined above, as they face the materiality of isolation and the deaths caused by the virus. The latest figures on the disease show that poor families are the most severely affected, with almost double the mortality rate.[15] In Brazil, the exception in terms of how marginalised territories are unserved by the state, and how inequality becomes ordinary—materialised in one of the highest death tolls in the world—seems to be the norm.

References

1. There are 13.5 million people in Brazil living on USD 1.9 per day. See: https://agenciadenoticias.ibge.gov.br/en/agencia-news/2184-news-agency/news/25895-extreme-poverty-affects-13-5-million-persons-and-hits-highest-level-in-seven-years

2. See: https://www.ibge.gov.br/en/statistics/social/population/18391-2010-population-census.html?edicao=19722&t=destaques

3. See: https://www.theguardian.com/world/2020/mar/25/bolsonaro-brazil-wouldnt-feel-anything-covid-19-attack-state-lockdowns

4. See: https://www.theguardian.com/world/2020/apr/07/china-outraged-after-brazil-minister-suggests-covid-19-is-part-of-plan-for-world-domination

5. See: https://www.wsj.com/articles/coronavirus-sweeps-across-brazil-a-land-ill-equipped-to-fight-it-11588603847

6. At the time of writing this note in June 2020, the Minister of Health was sacked by the president because of opinion clashes over Bolsonaro's position in underestimating the crisis. See: https://www.theguardian.com/world/2020/apr/16/bolsonaro-brazil-president-luiz-mandetta-health-minister

7. See: https://www.nbcnews.com/tech/social-media/facebook-removes-video-brazilian-president-endorsing-unproven-antiviral-drug-n1172566

8. See: https://www.theguardian.com/world/2019/oct/30/whatsapp-fake-news-brazil-election-favoured-jair-bolsonaro-analysis-suggests

9. See: https://www.bbc.com/worklife/article/20200309-coronavirus-covid-19-advice-chinas-work-at-home-experiment

10. See: https://educacaovigiada.org.br

11. See: https://www.brasildefato.com.br/2020/03/27/congress-approves-assistance-of-r-600-that-could-benefit-24-million-informal-laborers

12. See: https://www.brasildefato.com.br/2020/03/31/to-fight-the-crisis-entities-defend-taxing-the-rich-foreseeing-r-270-billion

13. See: https://casafluminense.org.br/organizacoes-e-liderancas-da-baixada-fluminense-lancam-manifesto-cobrando-medidas-de-prevencao-ao-coronavirus

14. See: https://www.mstbrazil.org/news/solidarity-food-settlements-poor-neighborhoods-homeless-people and https://www.mstbrazil.org/news/donations-acts-live-broadcasts-marked-launch-emergency-plan-people%E2%80%99s-agrarian-reform

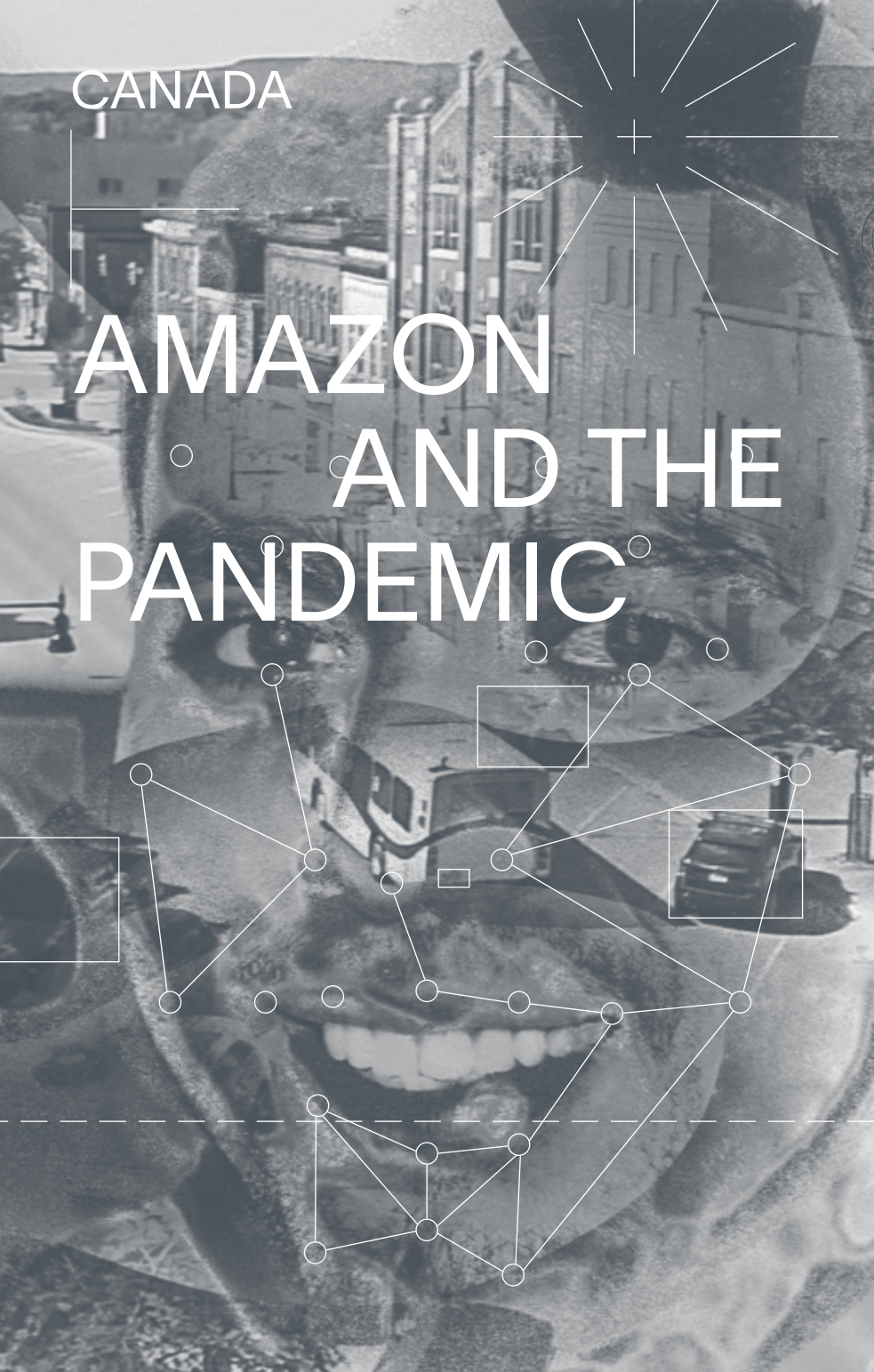
15. See: https://www.theguardian.com/world/2020/jun/09/enormous-disparities-coronavirus-death-rates-expose-brazils-deep-racial-inequalities

Rafael Evangelista is a researcher at Universidade Estadual de Campinas and founding member of the Latin American Network of Surveillance, Technology and Society Studies (LAVITS).

Rodrigo Firmino is an associate professor at Pontifícia Universidade Católica do Paraná in Curitiba, Brazil, and founding member of LAVITS.

CANADA

AMAZON AND THE PANDEMIC



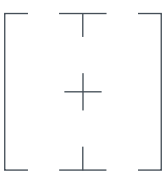
PROCUREMENT

RESPONSE

Bianca Wylie

To support rapid policy responses to the pandemic, governments around the world are working with the private sector in a range of ways: from factory conversions for medical gear and technology development to quick regulatory approvals and supply chain interventions. There is a lot of public interest on the table, and it is all happening fast.

In early April 2020, Justin Trudeau, the Prime Minister of Canada, made an announcement about a COVID-19 contract that the federal government had signed with Amazon Canada. Three features of this procurement stand out as notable: a lack of information available to the public about what the contract contained, the government stating that Amazon was doing the contract 'at cost, not profit', and the reputational laundering that this deal does for Amazon through the legitimacy of the Canadian federal government at a time the company's treatment of its warehouse workers is making international headlines.



Lack of information about the contract

One of the major features of the announcement was how little information it contained. The Prime Minister said the government had 'signed an agreement with Amazon Canada to manage the distribution' of medical supplies, including 'masks, face shields, gowns, ventilators and test-kits.' But because the government failed to be clear about the role Amazon was playing, many people were immediately upset that Canada Post was not tasked with the job. Later in the day, the government put out a press release,[1] which included the following details:

> 'Amazon will work collaboratively with the Government of Canada to process and manage orders through its online Amazon Business store. Amazon will use its Canadian distribution network, including delivery partners Canada Post and Purolator, to deliver these supplies to provincial health authorities, hospitals and other government agencies across the country.'

Now the Amazon part of the deal appeared to be the use of the Amazon Business Store. In my correspondence with the Minister of Public Services and Procurement's Office, I received the following information about the tender process that led to the contract: 'Following a supplier call-out issued by Public Services and Procurement Canada on March 12, 2020, a large number of suppliers offered assistance to support Canada, including Amazon Canada.' Which means the deal was done in close to two weeks. The Minister's office also honed in on the logistics capacity of the Amazon Business Store, describing the contract as covering: 'options to best manage the shipping, receiving, order processing, and distribution of personal protective equipment across the country.' Their email also indicated that they had contacted other suppliers, and that 'speed of deployment' was a factor in their selection of Amazon as the preferred vendor. I did not receive any information about the dollar amount of the contract, though I asked.

Less than two weeks following the announcement, PressProgress, a Canadian news outlet, wrote a piece that uncovered more of the same persistent problem with tech procurement and government: secrecy.[2]

As PressProgress reported: "Public Service and Procurement Canada (PSPC), the department in charge of awarding government contracts, refused to disclose the full terms of Amazon's contract with the Public Health Agency of Canada (PHAC). 'The contract between the Government of Canada and Amazon contains third party information protected under the Access to Information Act and the Privacy Act,' a PSPC spokesperson told PressProgress."

A deal done 'at cost, without profit'

In the government press release that followed the announcement, it was stated that Amazon Canada was providing the contracted services at cost, not profit. So here are a few more questions—the first one being, who assesses that Amazon Canada is providing something at cost? If this is the use of Amazon's platform, does this mean free or discounted licensing? But the next question lurking here is, what is Amazon Canada getting access to through this deal? Particularly, what data, digital architecture, and systems information is it getting access to? What is the value of knowing about the federal government's operations throughout this crisis? How about the logistics information of the partners involved? Are considerations such as these being factored into the deal or contract at all?

Further, with technology, there are known issues with something being provided 'at cost' to governments, which could mean anything from a discount to being close to free. When governments begin to use tech systems under these conditions, they often become entrenched infrastructures which are very difficult to remove. Big Tech firms, such as Amazon, are so highly capitalised that they can do many things at cost, or at a loss, if it will enable the company to become entrenched in a long-term way as public infrastructure. Or if it will help the company attain the legitimacy needed to operate in a new market space such

as healthcare. Our procurement systems have little to no defence against such strategic interventions; it is not how public procurement policy functions.

In terms of this deal being done 'at cost', so much boils down to the unknowns. What is cost? What is the government getting? What is Amazon Canada getting access to? What is its value? Is there a system of infrastructure being set up in this crisis context that will do more than this one project, and that will live on and past it?

Reputational laundering for Amazon

Finally, and likely the hardest to measure but of definite note and import, is the legitimacy that this kind of transaction lends to Amazon Canada, and how it positively impacts its brand. One jarring detail about the timing of the government announcement was that it came right on the heels of the news of Amazon executives denigrating one of their workers who was raising safety concerns for warehouse workers in
3 the context of COVID-19.[3] Here was a company that was not doing the right things for its own workers' safety in the US, but the Canadian government was more than happy to hold them up as helping partner with our country—sharing that they were doing a contract with Canada at cost, not at profit, as though it was doing us a favour. This hypocrisy has only gotten worse in recent days, with news of a VP at Amazon resigning due to the culture of fear the company was trying to create to stop whistleblowers and labour organisers who
4 wanted safer working conditions.[4]

This procurement and contract highlights several key issues that are surfacing persistently in this moment: tech actors potentially entrenching themselves in public systems and as public infrastructures through public tenders, the legitimacy that governments confer to tech companies, a lack of government awareness for the value of the public data they hold and
 their lack of valuation of our public systems, the ways that free or cheap services can game procurement systems, and how these advantages are used though the highly capitalised and patient advance of Big Tech.

References

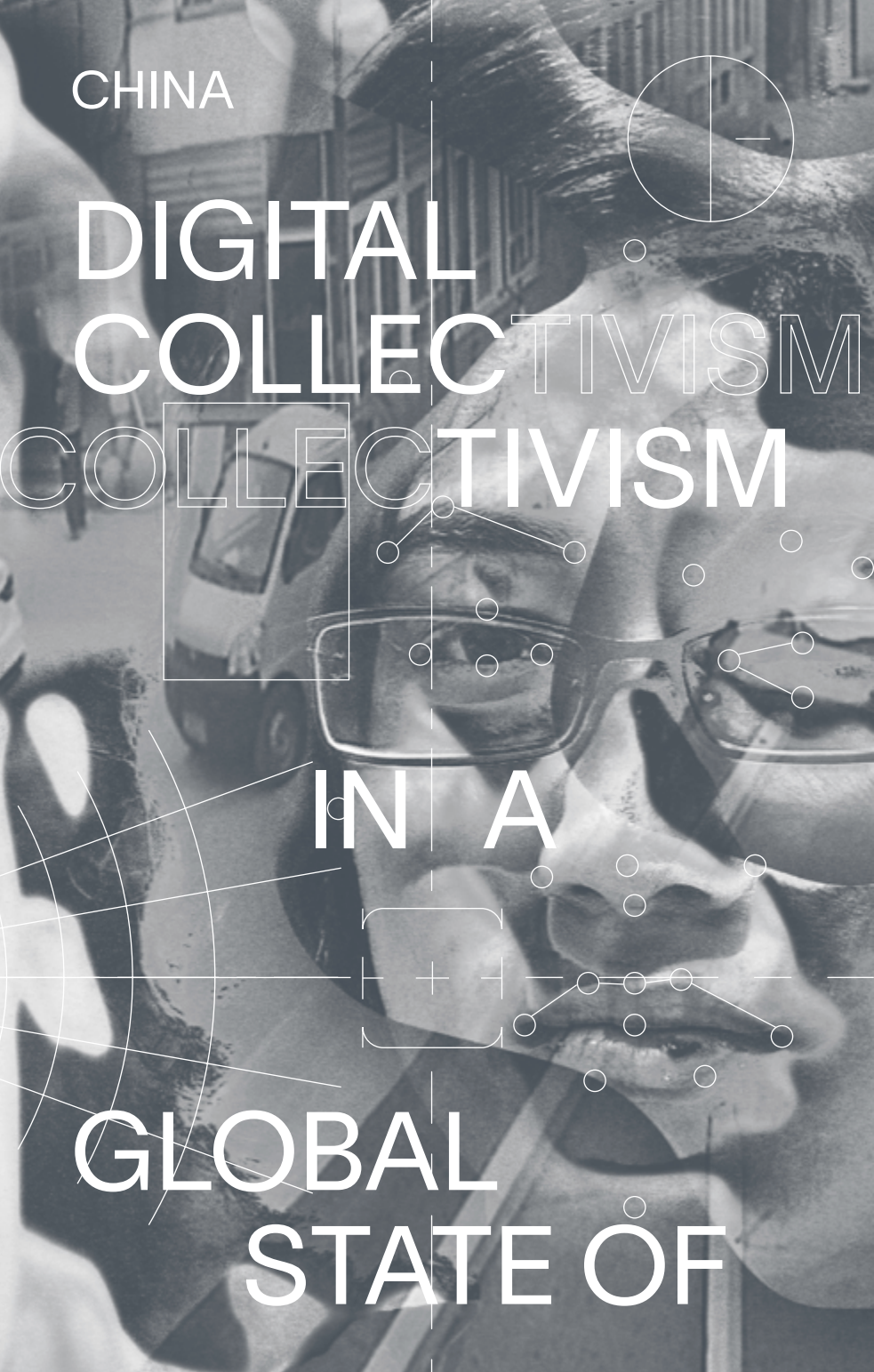
1. See: https://www.canada.ca/en/public-services-procurement/news/2020/04/government-of-canada-partners-with-amazon-to-help-get-personal-protective-equipment-to-frontline-healthcare-workers.html

2. See: https://pressprogress.ca/federal-government-wont-disclose-details-of-new-contract-with-amazon-to-manage-canadas-covid-19-supplies

3. See: https://www.theguardian.com/technology/2020/apr/02/amazon-chris-smalls-smart-articulate-leaked-memo

4. See: https://www.cbc.ca/news/business/tim-bray-quit-amazon-web-services-activist-employees-1.5555266

Bianca Wylie is a co-founder of Tech Reset Canada and a senior fellow at the Centre for International Governance Innovation.


CHINA
DIGITAL
COLLECTIVISM
COLLECTIVISM
IN A
GLOBAL
STATE OF

EMERGENCY

Wayne W. Wang

Francis Fukuyama has hypothesised that it is not the dichotomy between autocracies and democracies, but 'the state's capacity and, above all, trust in government' that determine a country's resistance to the coronavirus.[1] In this regard, China has shown its diverging approach to gaining public acceptance of, and trust in, the state's use of digital technologies by magnifying patriotism and nationalism. This dispatch discusses the role of the Chinese state and technology industry in the country's response to the COVID-19 crisis. First, it reveals how digital technologies have been employed to reduce coronavirus risks. Second, it explains how public–private partnerships in China, in which the bargaining power of private stakeholders has long been weak in the face of the administration, have intensified public information asymmetries through increased censorship and reinforced the state's capacity to mobilise society for wider coordination and compliance. Third, it comments on the role of digital collectivism that prioritised security over privacy in the Chinese response to the epidemic.

1

Authoritarianism, digital technology, and COVID-19

Following the soaring number of global confirmed cases from around March 2020, some began to debate whether authoritarianism might work better than democracy in managing states of emergency.[2] However, in this instance, China's large-scale use of advanced technologies (e.g. AI)—viewed as an essential part of Beijing's China Dream[3]—has also raised concerns about how public authorities might use the pandemic response as an opportunity to make permanent certain uses of digital technology. Permanent health tracking on smartphones was reportedly on the policy-making agenda of the Chinese local government.[4] The Chinese government and domestic companies have long been questioned about

2

3

4

patterns of technological social governance, including facial recognition,[5] online censorship,[6] the social credit system,[7] and social media.[8] However, in the form of accumulated innovation, these technologies also represent substantial measures in the fight against coronavirus by helping to predict outbreaks, offering online medical consultations, and ensuring timely deliveries of food and medicines.[9]

Information quarantine

The Great Firewall of China distinguishes between those who can cross the wall in order to access blocked content (e.g. via VPN) and those who cannot, leading to diverging levels of information freedom and thus shaping the spectrum of Chinese ideology.[10] Whether people are supportive (advocates), afraid (the self-censored silent and/or the unconscious) or sceptical (dissidents) of the propaganda on censored websites and platforms may depend on the amount of information they can receive from outside. Epidemiological statistics and the official narratives were promoted to secure social stability, while the blocked content outside the wall was regarded as a source of panic, unrest, non-coordination, and politically incorrect information.

The death by coronavirus of Dr. Li Wenliang, the COVID-19 whistleblower, drew much attention to the issue of freedom of speech in China.[11] Domestic public sentiment was both critical and complementary of the swift English translation of *Fang Fang's Wuhan Diary,* a collection of her Weibo posts. The diary was viewed simultaneously as ammunition for Chinese conspiracy theorists who believed its rapidly translated entries were meant to harm the country's reputation abroad, as well as a vivid record of Wuhan's social vicissitudes during the lockdown.[12] Social media platforms that algorithmically prioritised posts favourable to the Chinese state showed netizens the successful role of state power in impeding the pandemic and created a patriotic / nationalist climate as people internalised the interests of the state as their own good.[13]

Other countries' frameworks of privacy and data protection force the Chinese tech giants to tacitly practice 'One App, Two Systems' (OATS), where those with Chinese real-name identifiers (e.g. phone numbers and banking accounts) are subject to closer censorship than those with foreign ones. The Chinese government shows increasing tolerance for the unwritten OATS practice because a digital economy with a focus on consumer privacy has become a forceful driver of economic growth at the national level, only if the practice is irrelevant to cybersecurity broadly defined as a component of public and national security.[14] This constructs and underpins a utilitarian notion of technology focusing more on developmental targets and national / collective interests, rather than civic and individual rights.

14

Rhetorics of collectivism

Chinese collectivism implies that in the face of a state of emergency all citizens have a social and political responsibility to safeguard national security, and thus to abandon some fundamental rights. In this regard, digital technologies are playing a dominant role in both strengthening public trust in government and also in enforcing punishment, particularly when the core leadership of the Chinese government has technocratic tendencies.[15] During the pandemic, the centralised epidemic management prioritised security over privacy, while the regulatory environment was geared to data aggregation and sharing between public authorities and the private sector.[16] However, the administrative hierarchy involved in approving epidemiological disclosure features centralisation and collectivism, which may lack flexibility but does comport with public credibility. For instance, the top-down flow of information helped to avoid public panic and misinformation about COVID-19.

15

16

The Chinese Law on the Prevention and Control of Infectious Diseases outlines the epidemic information disclosure system to be established by the state. In principle, the State Council's health administration department can issue epidemiological announcements, or it can authorise the provincial health administration department to issue them. Although the data categories such announcements should disclose are unclear in the provision, the crowdsourcing datasets created by

online platforms (e.g. Dingxiangyuan and Tencent) allow provincial-level, municipal-level and district-level monitoring of tests, confirmed cases, recovery and mortality rates, and comprehensive news reports. Once the local health administration departments released those announcements, China's data scientists utilised their expertise to inform the public of the epidemiological trends and tolls almost in real time, along
17 with data-driven maps.[17] This expertise has been shaped by China's recent experience of immense datafication: it has
18 been described as 'the Saudi Arabia of Data'[18]—that is, a country with vast pools of data derived from the population's use of digital technology.

Finally, in the face of a pandemic, the Chinese public bore a collective responsibility for weighing procedural justice against technological efficiency—and arguably, success in legitimising or justifying technological interventions is not necessarily subject to moral, ethical, and behavioural acceptance and implementation of normative values. We may agree that normative values are deeply rooted in regional cultures and historical vicissitudes; and in this particular case, most Chinese people might consider individual rights as a worthwhile trade-off for the state's interests, because the state has been conceptualised as a collective community where all lives are bound and intertwined in the pandemic. We might ask ourselves what that trade-off looks like in democracies.

References

1. See: https://www.theatlantic.com/ideas/archive/2020/03/thing-determines-how-well-countries-respond-coronavirus/609025

2. See: http://www.bushcenter.org/publications/articles/2020/04/democracy-talks--covid-19--authoritarianism--and-democracy and https://www.economist.com/leaders/2020/04/16/is-china-winning

3. See: https://www.thechinastory.org/yearbooks/yearbook-2019-china-dreams/chapter-5-ai-dreams-and-authoritarian-nightmares

4. See: https://www.wsj.com/articles/chinas-plan-to-make-permanent-health-tracking-on-smartphones-stirs-concern-11590422497

5. See: https://www.reuters.com/article/us-health-coronavirus-facial-recognition-idUSKBN20W0WL

6. See: https://citizenlab.ca/2020/03/censored-contagion-how-information-on-the-coronavirus-is-managed-on-chinese-social-media

7. Dai, X. (2020) Enforcing Law and Norms for Good Citizens: One View of China's Social Credit System Project. *Development.* 63(1) 38–43. https://doi.org/10.1057/s41301-020-00244-2

8. King, G., Pan, J., & Roberts, M. E. (2017) How the Chinese Government Fabricates Social Media Posts for Strategic Distraction, not Engaged Argument. *American Political Science Review.* 111 (3) 484–501.

9. See: http://www.thechinastory.org/coronavirus-and-techno-authoritarianism

10. See: https://www.merics.org/sites/default/files/2020-04/171004_MPOC_05_Ideologies_0_web.pdf

11. See: https://www.caixinglobal.com/2020-02-06/after-being-punished-by-local-police-coronavirus-whistleblower-vindicated-by-top-court-101509986.html

12. See: https://www.scmp.com/news/china/politics/article/3080531/coronavirus-chinese-writer-hit-nationalist-backlash-over-diary

13. Chen, Z., & Wang, C. Y. (2020) The Discipline of Happiness: The Foucauldian Use of the "Positive Energy" Discourse in China's Ideological Works. *Journal of Current Chinese Affairs.*

14. Pernot-Leplay, E. (2020) China's Approach on Data Privacy Law: A Third Way Between the U.S. and the E.U.? *Penn State Journal of Law & International Affairs.* 8(1) 49–117.

15. See: https://issues.org/perspective-the-benefits-of-technocracy-in-china

16. See: https://merics.org/en/report/tracing-testing-tweaking

17. See: https://hub.jhu.edu/2020/01/23/coronavirus-outbreak-mapping-tool-649-em1-art1-dtd-health

18. Lee, K. (2018) *AI Superpowers: China, Silicon Valley, and the New World Order.* Houghton Mifflin Harcourt.

Wayne W. Wang is a robot-like nerd debugging Greater China in the virtual world.

ESTONIA AND FINLAND

THE POLITICS

OF A PANDEMIC

Helen Eenmaa-Dimitrieva, Eneken Tikk,
and Mika Kerttunen

The lessons learned from COVID-19 are not only about virology. The pandemic has intensified the dilemma between human and material values in national politics and reiterated the bitter contestation over the world order.

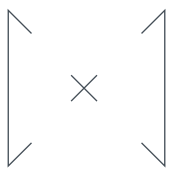
Estonia and Finland are small, rule-of-law abiding states. There are also historical and cultural similarities and ties between the two societies, to the point where people both in Estonia and Finland jokingly consider the social distancing more a normalcy than an exception in their social interaction. It is therefore not surprising that policies and decisions have not differed much between the two countries.

In some respect, the situation around the Gulf of Finland has not differed much from the rest of the world. We notice similar patterns of denial, confusion, and slow piecemeal decisions. And we have followed a similar trajectory to many other states: initial absentmindedness by public agencies about suitable measures, and attempts to downplay the effects of the virus on the population, soon followed by the realisation that the situation is much worse than originally thought. The Estonian and Finnish governments were both agile in declaring states of emergency, with powerful societal measures such as lockdowns and sheltering, closure of borders, and re-organisation of public and private operations. However, while the measures were decisive and forceful, they were still accompanied by denial and confusion from those in power.

Other developments have been of a more domestic character. Estonian society tends to be enthusiastic and impatient regarding the adoption of new technologies, but also noticeably attentive to minimising the accompanying risks. Due to its long history of occupations and a relatively recent memory of totalitarian rule, the Estonian population is particularly sensitive to any attempts at limiting personal liberties or steps leading to the loss of freedoms, e.g. freedom of speech, thought, assembly, and movement.

This impatient but security-focused attitude characterises Estonian reactions to the global pandemic as well as the adoption of new technologies for empowering individuals and governments operating within it. In a digital society, technologies are regarded as a natural element of society where matters of security, transparency, accountability, data protection, technological dependency, and competition regulation have both technological and non-technological components. However, with the crisis-led trend to adopt new technologies without observing the usual procedures of political debate and oversight, the pandemic has underlined the need to pay special attention to the acceptability of government as well as privately led measures.

In other matters, the same trends and patterns have been observable in both Estonia and Finland. We have seen public broadcasting companies and newspapers re-emerging as trusted sources of balanced and knowledge-based information when covering the domestic and international state of emergency. The reliance on and trust in public authorities has also increased. Particular authorities, obviously national health agencies and boards but also the chancellors of justice and the data protection inspectorates, have been at the forefront in providing advice and concrete recommendations in the debates about suitable measures for managing the crisis.



One such noticeable debate has focused on the question of whether Statistics Estonia (a public authority) could justifiably request private mobile operators to release their users' raw mobile phone tracking data for the government to gain an

overview of whether people's mobility patterns have changed as a result of the emergency measures. The debate involved several public authorities as well as all mobile operators, and focused predominantly on (1) the options for data sharing and (2) the potential danger that public authorities or members of present or future governments might find a way to abuse this. As a result of the deliberations, no raw data were released, and each private telecom carried out the analysis that the public authorities needed internally in compliance with data protection requirements, and Statistics Estonia received only the final results.

The pandemic has not only tested the healthcare system and standards but has also imposed a test of statehood. As a result, we may see greater attention paid to the functioning of governance systems and the effectiveness of public administration globally. This has certainly been true in Estonia and Finland.

Public authorities have, in general, followed expert opinion, initially of the medical and legal professionals and increasingly of the economic and security ones. Similarly, the crisis has underlined the political importance of scientific knowledge, especially that of virologists and other medical professionals with different statistical evidence and predictions. As the costs of governmental measures have become clearer, we also see more attention paid to national economists. In Estonia and Finland we can see that these respective value propositions and their practical applications have partially merged, resulting in a reopening of the societies and borders.

The collection, sharing, and analysis of data across society has also intensified under pandemic conditions. The trend that used to be justified with reference to improving the efficiency and quality of public services, now continues with suggestions to collect and analyse more private data in order to monitor, predict, and control the pandemic. These calls are most commonly led by computer scientists with a well-intended interest in helping with crisis management by offering more reliable research and statistics. Whether these calls should be followed or not, the pandemic has

reiterated the importance of the availability, relevance, and reliability of data. In Estonia, it has encouraged investment in ad hoc national data enhancement, such as the Estonian Cyber Defence League being deployed to assist the Estonian Health Authority. Along with that, it has reiterated the value of international institutions (like the World Health Organization) and global cooperation in such contexts.

All in all, COVID-19 has presented governments with hard choices between the life and the well-being of populations. The pandemic has tested not only crisis management and healthcare systems but also offered the much deeper challenge of preserving and promoting fundamental rights and freedoms. Amidst the global pandemic, we have been witnessing an intensified bifurcation between two competing value propositions: a human and a material one. The human proposition emphasises the quality of and the right to human life, including good care. The material one emphasises the economy. The proliferation of the virus has shifted governmental focus from the latter to the former. The shift has taken place through a re-organisation of businesses, reprogramming in working and private lives, testing of the public sector's operational capacity, and the emergence of new opinion leaders. That said, both Estonia and Finland have emerged from this challenge on the human side—placing human rights and fundamental freedoms over economic considerations.

The pandemic has also highlighted one entirely different dimension. For small countries like Estonia and Finland, international order and the sense of an international community are crucial. However, the global sense of urgency, even panic and dystopian depression, has led governments and the public to return to nostalgia, nationalism, and protectionism. This has manifested in calls for renewed reliance on national capacity, e.g. domestic production, domestic or like-minded supply chains for cash, medicine, equipment, and spare parts. The crisis seems to have drawn global attention away from climate change and environmental protection, and invigorated discriminatory and xenophobic tendencies in places where we believed these to have been abolished. The pandemic has also underscored that states'

modi operandi and prevailing ambitions are unlikely to change during a crisis. For example, the United States' accusations against China and cutting of funding to the WHO continue the trend of US exceptionalism and unilateralism. This shows how emergency decision-making continues to reveal the tendencies and priorities of executive power—pragmatism and expediency certainly, but also opportunism and unilateralism. Without societal and political resilience, there is a danger that crisis-mentalities become the new normal.

The global emergency has imposed restrictions and reduced freedoms in all countries. In societies where such restrictions are already common, the change has been least disruptive. In countries where such restrictions are temporary and need-based, success will be measured by the return to normalcy of fundamental rights and freedoms. The task for liberal democracies is to ensure that technological advances and innovation remain the source of economic and societal benefits, rather than becoming a new means of governmental control. That said, crises also present an opportunity to re-organise societies and renew societal processes—those leading on these fronts might turn out to be the greatest winners of all.

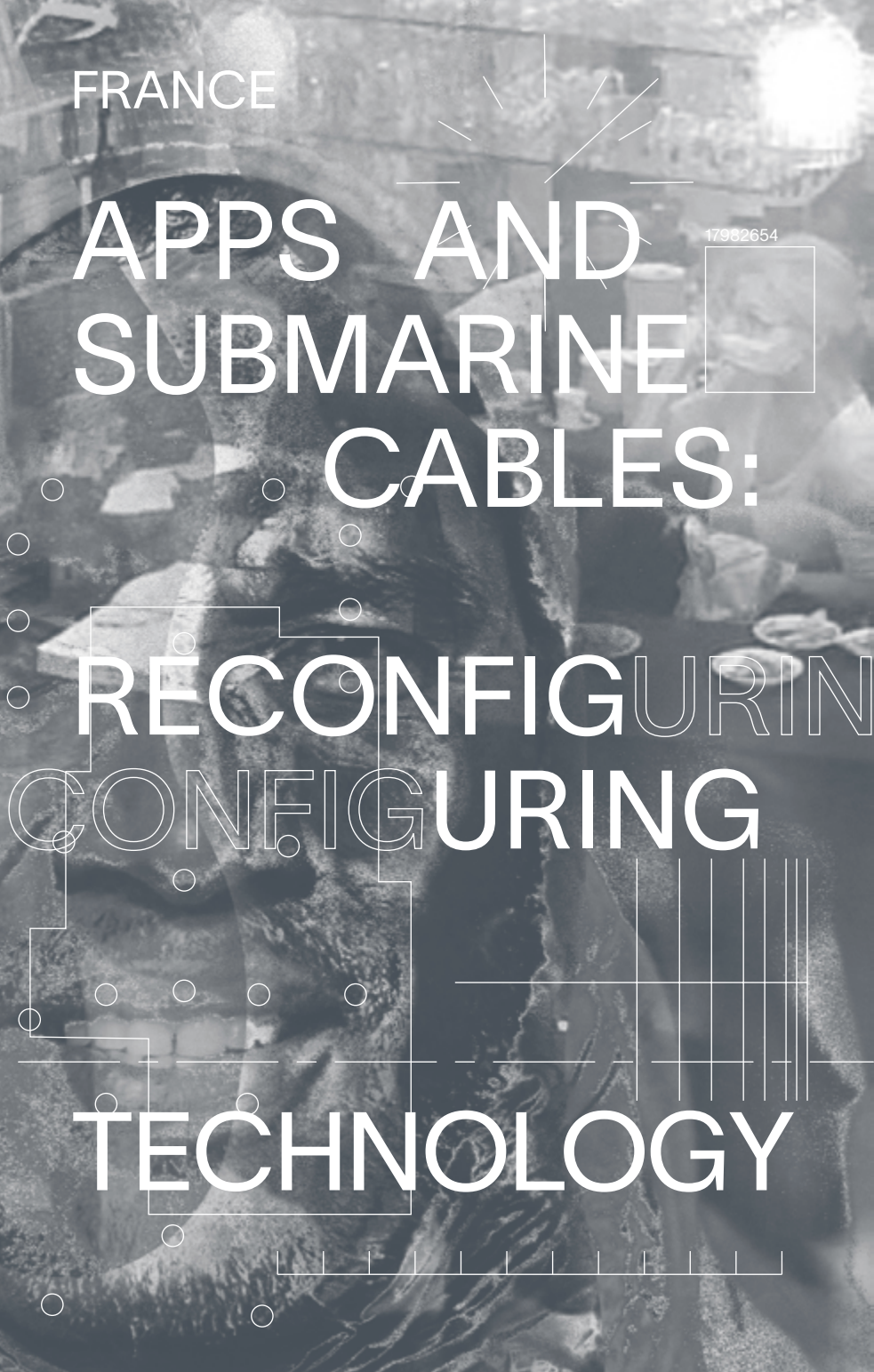
Helen Eenmaa-Dimitrieva is a researcher in information technology law at the University of Tartu, Estonia and a member of the Estonian Young Academy of Sciences.

Mika Kerttunen is research scientist at Tallinn University of Technology, Estonia.

Eneken Tikk is research scientist at Tallinn University of Technology, Estonia. Mika and Eneken are co-editors of the Routledge Handbook of International Cybersecurity.

FRANCE

APPS AND SUBMARINE CABLES: RECONFIGURING TECHNOLOGY



IN A STATE OF URGENCY

Francesca Musiani

This piece provides an overview of the main issues that are currently being discussed in France, and highlights some of their implications for the (re-)distribution of authority mediated by digital technology. A first, perhaps central, theme of debate is the use of big data, in particular personal data, to counter the pandemic. Since the beginning of the epidemic worldwide, initiatives related to this aspect were either envisaged or implemented in a number of countries, with a shared rationale:[1] COVID-19 propagates with people moving around, thus, using the massive digital data generated by our smartphones can both help in understanding the ways in which the virus progresses and guide political decision-making on social distancing and confinement.

1

In France, this rationale gradually took shape as the StopCovid project, a smartphone application meant to 'limit the spread of the virus by identifying transmission chains', monitoring social relations of users to warn at-risk individuals—as Olivier Véran and Cédric O, the Ministers of Health and Digital Affairs, explained in early April to
2 France's foremost newspaper, *Le Monde*.[2] While the two officials mentioned that they were in an 'exploratory phase, while exploring all possibilities', they could initially count on widespread support from the French population: a late-March survey conducted in France on behalf of University of Oxford researchers showed that eight individuals out of 10 would be in favour of installing such an application, with two thirds mentioning that they would even be in favour of an automatic installation by phone operators (an option which, in any case,
3 was technically infeasible).[3] This popular support would subsequently falter, as more debates took place on the app
4 project and its potential weaknesses were uncovered.[4]

Perhaps unsurprisingly, StopCovid—and more generally the possibility to use big data, surveillance, and geolocalisation to fight COVID-19—was from the start the subject of much controversy. Threats to privacy were an important concern, with CNIL (the French Privacy and Data Protection
5 Commission) emphasising in a March 25 recommendation[5] that such a project should 'privilege the treatment of anonymised data rather than individual data' (with the well-known
6 difficulty of truly and fully anonymising data),[6] and in the cases when an individual follow-up would be necessary, it should be based on a 'voluntary action of the concerned person'. Discussions of the more or less problematic character of the app for civil liberties were mostly linked to discussions about its technical features, in particular
7 data storage modalities:[7] How would data be protected?

Would there be a centralised file and, if yes, who would maintain it? Preliminary reports indicated that the French government, advised by a task force led by Inria, the French national research institute for the digital sciences, was privileging solutions centred on Bluetooth rather than on
8 GPS,[8] thereby prioritising technological solutions considered as less intrusive, the most cited example of which was Singapore's TraceTogether.

Another concern linked to this application was its effectiveness, with tech journalist Hubert Guillaud interestingly pointing out that the app was bound to suffer from two problems:[9] transforming a 'sign' into a 'signal' (i.e. reading proximity with an ill individual as an anticipation of infection so as to trigger an alert and a treatment), and, in a likely-prolonged state of urgency, turning what should only be a brick in a wall of preventive measures into the only recourse of France's COVID-19 health policy. Finally, a more meta-concern, vehemently voiced by digital liberties associations such as La Quadrature Du Net,[10] was the temporal dimension: if specific surveillance and data processing initiatives are authorised in a state of urgency, and under particular conditions—will we be able to go back, how, and to what extent?

Initially envisaged as a companion to the set of deconfinement measures implemented from May 11, the StopCovid application was officially released on June 2, and made available in Apple's and Google's online stores.[11] A week later, on June 9, the Ministry of Digital Affairs announced that the app had been downloaded *and* activated by 1.4 million French citizens, about two percent of the total population—an adoption rate considered disappointing by the government, which was hoping to be able to count on numbers similar to Australia's (8%) and Norway's (25%) to improve the effectiveness of StopCovid (a critical mass of users must be reached for the results to be meaningful).[12] Given that effectiveness is one of the primary conditions for the CNIL to maintain its support for the app project even in light of its potential privacy risks,[13] StopCovid's promoters are concerned, but do not yet wish to draw conclusions about its success; more information will be needed about the number of actually *active* users (a first estimate indicates around 350,000), the geographical disparities of use (urban vs rural especially), and the number of alerts sent as well as their correlation with the carrying out of tests.[14] Nonetheless, the limited number of downloads and notifications so far has led several voices to speak of a predictable fiasco,[15] and to express concern about the seemingly disproportionate hosting and maintenance costs for the app, which, after a phase of development driven by 'national solidarity', would now burden the state.[16]

While this debate continues to be the liveliest one concerning issues of technology and authority in France, several others that touch more broadly on tech justice can be identified. One concerns the sustainability of Internet infrastructures due to the massive shifts in both work habits (a steady increase of remote working practices) and the perusal of digital content for leisure. Orange, France's historical operator and Internet service provider (previously France Télécom) quickly announced it would be doubling the capacity of submarine cables that connect it to the United States (thus, connecting French users to Silicon Valley services, representing 80% of the nation's traffic).[17] However, French data centre operators warned that the capacity to receive such traffic depends on the quantity of servers set up by companies,[18] with several reporting to have underestimated the burden and others announcing that they would impose access restrictions.[19] Linked to this issue was the debate on the digital responsibility of individual citizens / Internet users, who were called upon to avoid imposing excessive loads on mobile networks (e.g. Fédération des Télécoms's secretary general launching a Twitter hashtag #TousEnWifi on March 19, asking for the public to favour WiFi connections over 4G).[20]

A final issue connected to tech justice concerns the infrastructure and practices of remote working, as catalysts of (more or less digital) inequalities. In particular, the French press has published a number of articles exploring the inability of several socio-professional sectors of the French population to work or learn from home,[21] either due to infrastructural / material constraints or to the fact that their professions cannot be exercised remotely, thereby putting them at greater risk of illness. The Covid-19 pandemic, and the 'going all-digital' shift it entails, are understood as accelerators of social exclusion—historically referred to as the digital divide—for primarily three groups of people: 'the young, for financial reasons; the elderly, for lack of interest, they say; and the rural world, which is partly explained by questions of quality of the network and equipment'[22]—a dynamic that has reminded the nation that half of those living outside the largest cities in France consider the quality of their Internet connection to be unsatisfactory.

Like in most countries worldwide, the COVID-19 pandemic in France is posing a number of challenges that are in some respects unprecedented, at least since our world has become a pervasively digital and networked one. But the tools to study surveillance, risk, inequality, and justice that we have been building as scholars and citizens for a long time can be of use to start trying to make sense of all that is happening.

References

1. See: https://www.lemonde.fr/pixels/article/2020/03/20/contre-la-pandemie-de-nombreux-pays-misent-sur-la-surveillance-permise-par-le-big-data_6033851_4408996.html

2. See: https://www.lemonde.fr/planete/article/2020/04/08/stopcovid-l-application-sur-laquelle-travaille-le-gouvernement-pour-contrer-l-epidemie_6035927_3244.html

3. See: https://www.lemonde.fr/pixels/article/2020/04/01/coronavirus-les-francais-favorables-a-une-application-mobile-pour-combattre-la-pandemie-selon-un-sondage_6035233_4408996.html

4. See: https://www.lindependant.fr/2020/04/12/une-majorite-de-francais-contre-une-application-obligatoire-de-type-stopcovid-sur-leur-telephone,8843795.php

5. See: https://www.mediapart.fr/journal/france/250320/surveillance-de-l-epidemie-la-cnil-met-en-garde-le-gouvernement

6. De Montjoye, Y.A., Hidalgo, C.A., Verleysen, M., & Blondel, V.D. (2013) Unique in the crowd: The privacy bounds of human mobility. *Scientific Reports.* 3, 1376.

7. See: https://www.lemonde.fr/idees/article/2020/03/20/les-libertes-publiques-a-l-epreuve-du-covid-19_6033764_3232.html

8. See: https://www.mediapart.fr/journal/france/090420/le-gouvernement-se-dirige-reculons-vers-un-pistage-massif-des-francais

9. See: https://medium.com/@hubertguillaud/stopcovid-le-double-risque-de-la-signose-et-du-glissement-b1e2205bff5a

10. See: https://www.laquadrature.net/2020/03/19/contre-le-covid-19-la-geolocalisation-deja-autorisee

11. See: https://www.economie.gouv.fr/stopcovid

12. See: https://www.lemonde.fr/pixels/article/2020/06/10/l-application-stopcovid-connait-des-debuts-decevants_6042404_4408996.html

13. See: https://www.cnil.fr/fr/la-cnil-rend-son-avis-sur-les-conditions-de-mise-en-oeuvre-de-lapplication-stopcovid

14. See: https://www.lemonde.fr/pixels/article/2020/06/10/l-application-stopcovid-connait-des-debuts-decevants_6042404_4408996.html

15. See: https://www.europe1.fr/economie/stopcovid-pourquoi-le-fiasco-etait-previsible-3974352

16. See: https://www.numerama.com/business/629585-stopcovid-le-cout-dhebergement-de-lapplication-de-tracage-des-contacts-fait-polemique.html

17. See: https://www.01net.com/actualites/orange-double-ses-capacites-de-connexion-avec-les-etats-unis-pour-faire-face-a-la-demande-1881488.html

18. See: https://www.lemagit.fr/actualites/252480352/Teletravail-les-reseaux-tiennent-le-coup-pas-les-services

19. See: https://www.nextinpact.com/brief/equinix-ferme-l-acces-a-ses-sites-ibx-notamment-en-france-11726.htm

20. See: https://www.01net.com/actualites/petit-guide-des-bonnes-pratiques-numeriques-en-temps-de-coronavirus-1878014.html

21. See: https://www.mediapart.fr/journal/france/180320/le-teletravail-un-miroir-des-inegalites-numeriques?onglet=full and https://www.lemonde.fr/education/article/2020/03/17/coronavirus-et-enseignement-a-distance-entre-augmentation-des-inegalites-educatives-et-transformation-pedagogique_6033349_1473685.html

22. See: https://www.lemonde.fr/idees/article/2020/05/13/coronavirus-l-inegalite-devant-le-numerique-devient-un-facteur-majeur-d-exclusion_6039493_3232.html

Francesca Musiani is associate research professor at the French National Centre for Scientific Research (CNRS) and deputy director of its Centre for Internet and Society.


GERMANY
28346591
BUSINESS
AS
USUAL?

RESPONSES TO THE PANDEMIC

Ben Wagner

The debate on COVID-19 in Germany has been closely associated with the power of the technology sector. Most of the German debates in regard to the power of technology are associated with data protection, whereas other important aspects such as transparency, accountability, technological dependency or competition policy are not discussed to the same degree. Notably, there is a stronger than usual tendency in Germany (and elsewhere in Europe) to promote the local development of technology so that German companies profit from any economic benefits associated with technological development. It is also frequently suggested that technology development for COVID-19 is seen as a key strategic resource that cannot be allowed to leave the country. Importantly, the technological developments that we can see in Germany are not massively different than would otherwise be expected in less exceptional circumstances. Technological development during COVID-19 seems to be business as usual in Germany.

How is information about people who have tested positive for COVID-19 being shared?

Healthcare in Germany is organised at the level of federal states. As a result, each of the 16 states has a list of individuals who have tested positive within that state. It seems that lists of positive patients have been shared with police forces

in four states: Baden-Württemberg, Schleswig-Holstein,
1 Lower Saxony, and Bremen.[1] Beyond this, no lists of specific individuals who have tested positive seem to have been shared between individual states, or between states and the federal government. The state police forces in Hesse have
2 been using Palantir's Gotham product for several years,[2] and it seems plausible that through this system Palantir may also gain access to German patients' data. There has also been a broad public debate in Germany about privacy and data sovereignty concerns associated with government
3 agencies using Palantir.[3]

How is COVID-19 contact tracing being implemented?
Originally, Germany's contact tracing implementation was to be based on the Pan-European Privacy-Preserving Proximity Tracing (PEPP-PT) standard. PEPP-PT is a European initiative primarily driven by Hans-Christian Boos, the founder and Managing Director of Arago AG, a German IT
4 company.[4] A recent conflict between the Decentralized Privacy-Preserving Proximity Tracing (DP3T) standard, a privacy-protective technical approach for contact tracing, and PEPP-PT makes it unclear whether PEPP-PT will indeed provide a European framework for developing contact tracing. This conflict is because PEPP-PT pursues a centralised server-driven approach to users' records while
5 DP3T is focused on a decentralised client-based approach.[5] Privacy advocates have legitimately questioned the need
6 for any centralised server infrastructure at all.[6] This conflict led to wider questions about the maturity and quality of the software being developed by Arago AG in the context of PEPP-PT, raising the question of whether contact tracing
7 would be used in Germany at all.[7] In no small part because of this conflict, Germany abandoned PEPP-PT at the end of April 2020 and instead began developing an
8 app on the basis of the DP3T framework.[8] Beyond
136 D3PT and PEPP-PT, the German government is also considering using an app developed by Accenture and the Red Cross in Austria. Finally, the German Chaos Computer Club has published a list of 10 test criteria, based on which contact-tracing apps
9 should be evaluated.[9]

How is hospital resource management being implemented?

The German federal government has implemented a centralised hospital bed management system, in order to ensure that it has an overview of all hospital and ICU beds in the different federal states in Germany.[10] However, beyond this information no personal data about COVID-19 patients is shared between the central government and federal states. One notable exception to this is the state of Hesse. Separately from its police implementation of Palantir's Gotham software, Hesse now also intends to use Palantir's Foundry to respond to the current COVID-19 crisis.[11]

10

11

Additional new technologies used during the COVID-19 pandemic

Another notable technological implementation is the request for voluntary submissions of personalised health data by the leading German public health institute (similar to the Centers for Disease Control and Prevention in the United States), the Robert Koch Institute (RKI). For this purpose, the RKI has developed an app that is publicly available and requests gender, age, weight, height, health and activity data on sleeping patterns, heartbeat, and body temperature, and postcode.[12] It seems that, based on this data, the RKI is planning to develop algorithms that will attempt to guess whether a user is likely to have COVID-19 or not.

12

The development of technologies in Germany is going in numerous different directions, with so many actors involved that it is remarkably hard to predict how it will develop in future. Notably, there are no significant changes to existing patterns of technology and power that have developed due to COVID-19. Thus, while COVID-19 has provided a new case for the existing German technology-power matrix, it has not served to destabilise or question it. If anything, existing patterns of technological development and management in Germany have been replicated for a new challenge without significant innovation to be observed.

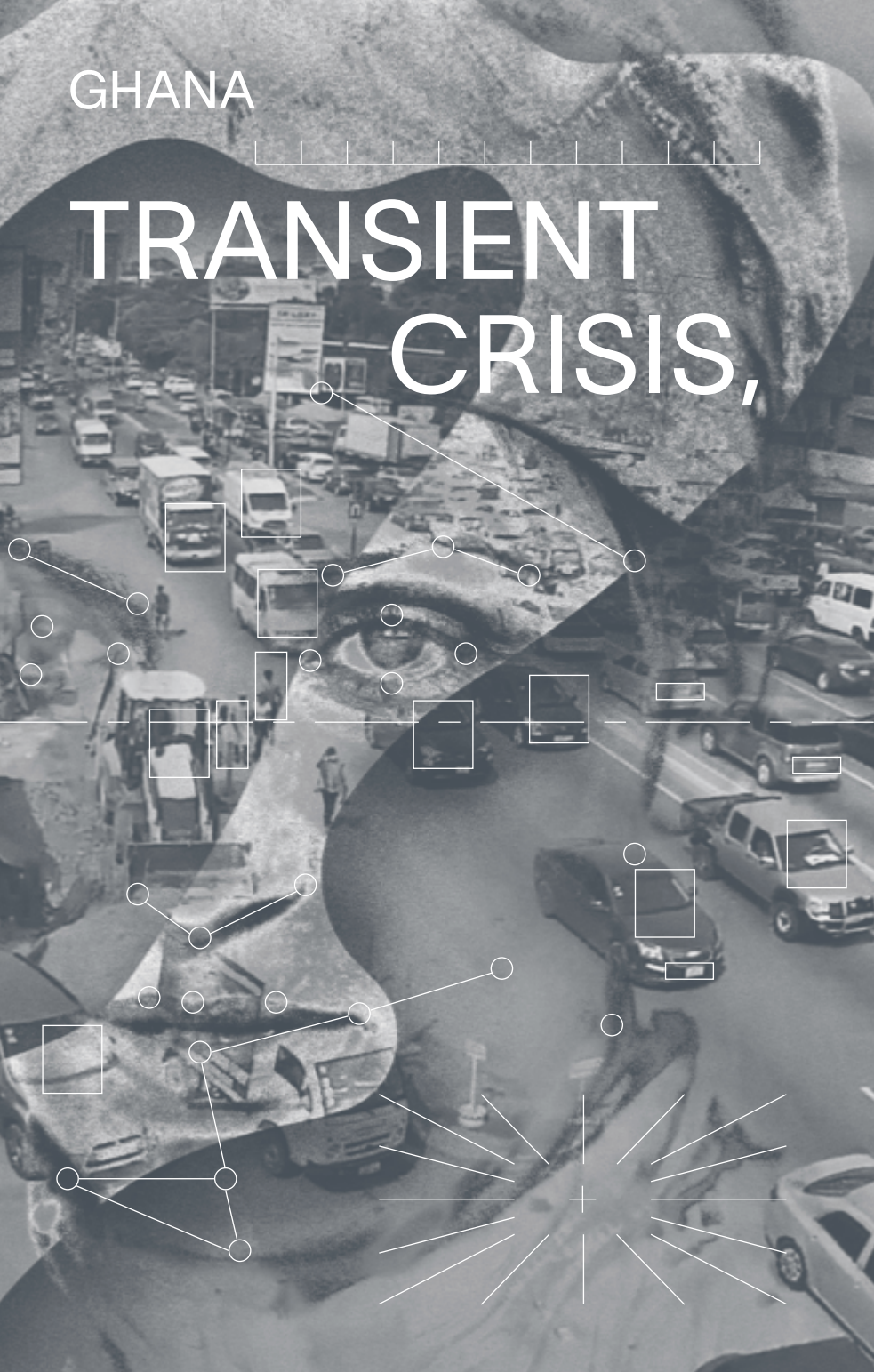
References

1. See: https://netzpolitik.org/2020/daten-von-infizierten-polizei-sammelt-in-mehreren-bundeslaendern-coronavirus-listen
2. See: https://www.sueddeutsche.de/digital/palantir-in-deutschland-wo-die-polizei-alles-sieht-1.4173809
3. See: https://www.neues-deutschland.de/artikel/1135061.corona-daten-bundesregierung-schweigt-zu-palantir.html
4. See: https://www.pepp-pt.org/impressum
5. See: https://nadim.computer/posts/2020-04-17-pepppt.html
6. See: https://www.telecompaper.com/news/german-govt-weighs-3-options-covid-19-tracing-app--1335550
7. See: https://www.chip.de/news/Corona-App-Diese-drei-Modelle-prueft-die-Bundesregierung_182637903.html
8. See: https://www.reuters.com/article/us-health-coronavirus-europe-tech/germany-flips-to-apple-google-approach-on-smartphone-contact-tracing-idUSKCN22807J
9. See: https://www.ccc.de/de/updates/2020/contact-tracing-requirements
10. See: https://rp-online.de/politik/kuenftig-meldepflicht-fuer-freie-intensivbetten-in-kliniken_aid-49937527
11. See: https://www.sueddeutsche.de/digital/coronavirus-hessen-foundry-palantir-1.4884568
12. See: https://www.rki.de/DE/Content/InfAZ/N/Neuartiges_Coronavirus/Corona-Datenspende.html

Ben Wagner is an assistant professor and director of the Privacy & Sustainable Computing Lab at Vienna University of Economics and Business.

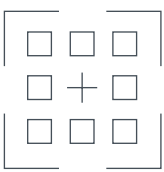
GHANA

TRANSIENT CRISIS,



PERMANENT REGISTRIES

Smith Oduro-Marfo



Increasingly, the COVID crisis has lent itself to surveillance systems and practices. In order to contain the spread of the virus, state and non-state actors around the world have invested in various surveillance tools, particularly for taking body temperatures and for contact tracing. In addition to a symptom-tracking app, the Ghanaian government has passed legislation to enhance the powers of the state over telecommunications systems during public emergencies.[1] In March 2020, the government passed Executive Instrument (EI) 63—the Establishment of Emergency Communications System Instrument, 2020.

1

EI 63 is partly justified by the state as a response to the 'urgent need to establish an emergency communications system to trace all contacts of persons suspected of, or actually affected by a public health emergency and identify the places visited by persons suspected of or actually affected by a public health emergency.'[2] Of course, with COVID-19 as a tangible reality, and the need for contact tracing as a presently popular mitigating measure, the basis of the EI seems sound. This is especially true in the case of countries like Ghana where SIM registration measures[3] have not been

2

3

entirely successful, and where the digital footprints of citizens are opaque. Thus, there is the prior (infrastructural) difficulty for African governments in terms of knowing who owns which phone, as well as with tracking, generally.

But what exactly would constitute 'an emergency communications system'? The EI instructs the establishment of a centralised registry for subscriber identity modules, and a centralised registry for mobile equipment identities. In other words, a national database that matches individuals to their phone numbers, and another that matches phone numbers to phone models, is now required by law. Mobile Network Operators (MNOs) are obliged by the EI to maintain an equipment identity register that will feed into the central registry. MNOs are also required to allow the state access to their networks for purposes of 'mass dissemination of information to the public in case of an emergency.' Thus, at first glance, the state should now know who owns what number and what phone, and this should make tracking phone use and users easier.

Practically, the COVID crisis has illustrated a certain kind of social legibility that the Ghanaian government requires to ensure citizens' healthcare, but does not yet have. However, through EI 63, the likely transient crisis has now been institutionalised as a 'permanent threat' that demands a corresponding permanent legislation.

Interestingly, the text of the EI strategically centres its provisions as responding to public emergencies, and quickly cites public health emergencies as only one example of such. In this sense, the state has basically exploited a public health crisis to legislate for all public emergencies. Worse, the EI does not define public emergencies. But understanding what constitutes a public emergency is crucial in appreciating when exactly telecommunications systems are to be left at the disposal of the state, and when the mobile phone registries are to be activated.

Naturally, the structures that are being mandated by the EI, including the registries for SIMs and equipment identities, are going to be more present and permanent than any

emergency. Without any sunset clauses, these mandated structures may occasionally be used as intended for mitigating emergencies, but could also be used for non-emergency surveillance practices in between.

More explicitly, the potential risks with EI 63 include: first, that the Ghanaian government could now be in a position to track communications of citizens in real-time. While this may be useful for national security purposes, in a country where security agencies are often at the beck and call of governmental actors, the arbitrary and self-serving use of such a surveillance system cannot be discounted. Second, without an explicit definition of public emergencies nor any clauses to restrict application of the EI to the COVID-19 crisis, the instrument is for the long term, legalizing potentially intrusive state surveillance structures that may have little to do with the current pandemic, or even with actual public emergencies. Critically, the instrument sidesteps existing legislation that makes the monitoring of personal communications by state and security actors, subject to a court warrant.

The aforementioned concerns about the EI have been raised in commentaries by civil society,[4] political actors,[5] and columnists[6]. A private citizen has also taken the matter to court.[7] One could hope that Ghana's Data Protection Act (2012) and the Data Protection Commission can act as some sort of bulwark in ensuring that these registries do not compromise data privacy and protection. However, per Article 60 of Ghana's Data Protection Act there are personal data processing and use exemptions, in the service of objectives such as national security and public safety.[8] Of course, public emergencies could easily qualify for these exemptions. This is possibly why there are hardly any notes in EI 63 on data privacy and security.

4, 5, 6

7

8

Probably, the best way to ensure that the telecommunication registries are not abused for purposes of arbitrary mass and micro surveillance by the state and the MNOs is to invoke Ghana's relatively stable democratic institutions. Here, the goal would be to ensure that the personal data in these registries are *only* used in scenarios that reasonably qualify as public emergencies. All told, it is in the interest of citizens if the state

has stronger informational capacity to respond to public emergencies. However, while public emergencies are typically a state of exception, EI 63 appears to be setting up permanent registries—and without the necessary safeguards, may therefore occasion a persistent threat to citizens' personal and data privacy rights, as well as their broader freedoms.

References

1. See: https://news.itu.int/ghana-launches-covid-19-tracker-app

2. See: https://ghanalawhub.com/establishment-of-emergency-communications-instrument-2020-e-i-63-a-dangerous-illegality

3. In the last decade or so, most African governments have attempted to make the registration of SIM cards compulsory for citizens and residents. SIM registration seeks to have a state-supervised registry that connects phone numbers with their users. However, these efforts have often not been successful. See for instance, https://www.biztechafrica.com/article/ghana-embark-re-registration-sim-cards-2020/15099

4. See: https://politicsafrika.com/index.php/2020/04/15/ei-63-is-unconstitutional-stranek-africa

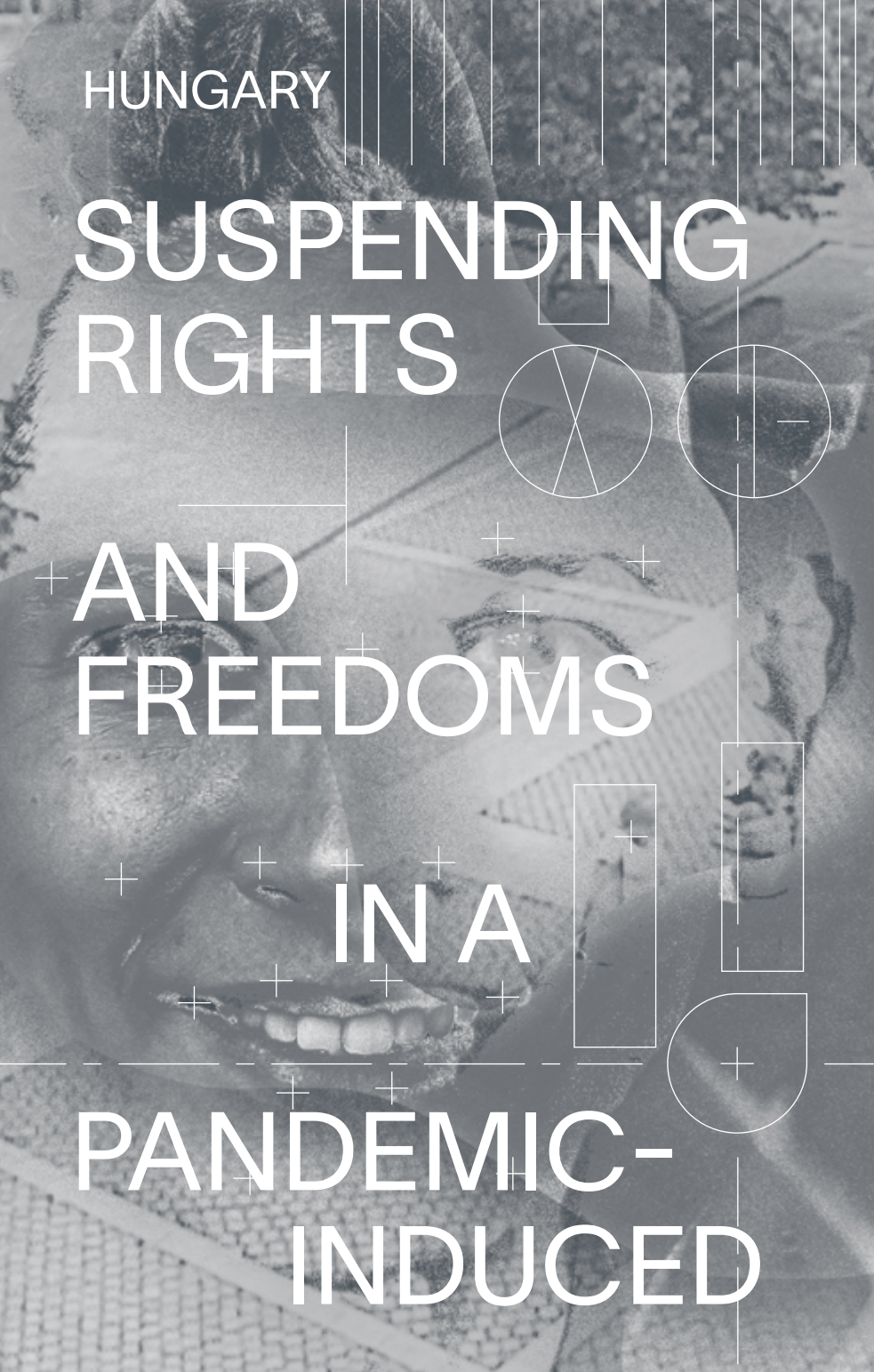
5. See: https://www.myjoyonline.com/news/national/we-resist-governments-attempt-to-hide-behind-coronavirus-pandemic-to-listen-in-on-our-phone-calls-ablakwa

6. See: https://citinewsroom.com/2020/04/kwaku-antwi-boasiako-un-learned-constitutional-interpretation-of-e-i-63

7. See: https://www.myjoyonline.com/business/telecom/lawyer-challenges-akufo-addos-attempt-to-secure-private-information-of-mobile-subscribers

8. See: https://dataprotection.org.gh/resources/downloads/data-protection-act/38-data-protection-act-2012-act-843/file

Smith Oduro-Marfo is a PhD candidate at the University of Victoria in Canada, focusing on the connections between surveillance and development in the Global South.



HUNGARY

SUSPENDING RIGHTS AND FREEDOMS IN A PANDEMIC-INDUCED

STATE OF DANGER

István Böröcz

Declaration of the state of danger

Article 53 of the Fundamental Law of Hungary empowers the government to declare a state of danger [1], 'in the event of a natural disaster or industrial accident endangering life and property, or in order to mitigate its consequences.'[2] Thus, in a state of danger derogations from the normal requirements of necessity and proportionality concerning interferences with fundamental rights and freedoms are possible, should they be necessary to tackle the particular danger but not otherwise.

On March 11, 2020 the Hungarian government declared a state of danger for the territory of the country in the 40/2020 Government Decree,[3] allowing the government to carry out its activities without the involvement of the National Assembly beyond reporting to it.[4] Whereas such an option is not unparalleled in European constitutional democracies, in Hungary the epidemic provided a unique opportunity for the Orbán regime[5] to continue its systematic demolition of European fundamental values, in particular the right to privacy and the freedom of information.[6]

On March 30, 2020 the National Assembly adopted the Act XII of 2020, which granted authorisation to the government to extend the applicability of its decrees adopted during the period of state of danger, in order to be able to take all extraordinary measures necessary for prevention. In particular, 'the National Assembly authorised the Government to extend the applicability of the government decrees under Article 53(1) and (2) of the Fundamental Law adopted in the state of danger

until the end of the period of state of danger.'[7] The state of danger lasts until the decision of the National Assembly,[8] but given that Viktor Orbán's party possesses a two-thirds majority in the National Assembly, the end date of the state of danger technically depended on his command. On June 18, the Act LVII of 2020 terminated the state of danger.[9]

Abolishing the rights of the data subject and freedom of information

To fight the coronavirus pandemic, on March 16, 2020 the 46/2020 Government Decree granted the Minister responsible for Innovation and Technology access to all data available without limitations, including the personal data of citizens.[10] Three weeks later, on April 6, 2020 the 93/2020 Government Decree allowed the operational staff, a body set up for the defence against the coronavirus,[11] to request and gain access to information from any organisation, legal entity or entities without legal personality in order to perform its tasks.[12] Furthermore, for the aforementioned purposes the operational body was also entitled to be informed about the persons affected by or suspected of having the coronavirus, as well as the persons in contact with them. Such information entailed among other things, personal identification data, contact information, health and register data. The operator of the National eHealth Infrastructure (Eletronikus Egészségügyi Szolgáltatási Tér, EESZT) also had to share all coronavirus-related information with the operational staff, including personal data.[13] Although access to information for the minister and the operational staff was guaranteed, limitations thereof and the details of the processing remained unaddressed.

The 179/2020 (May 4, 2020) Government Decree enacted changes in the application of the 2016/679 General Data Protection Regulation (GDPR) and its national implementation, the Act CXII of 2011 on Informational Self-Determination and Freedom of Information (Privacy Act) as well.[14] In particular, any activity, in connection with applications concerning the practice of the rights of the data subject (such as the right to information, rectification, erasure, objection, etc.)[15] were suspended until the end of

the state of danger.[16] To reiterate: a government decree of an EU Member State suspended the provisions of a directly applicable EU regulation. 16

Decisions of the government affected not only the right to the protection of personal data but also freedom of expression and information. Besides expanding the definition of the crime of scaremongering with a new behaviour ("impediment of defence against pandemic situation"),[17] requests for access to data of public interest and data accessible on public interest[18] could be submitted only in written form and shall be fulfilled not later than 45 days, instead of 15, with a possible extension for another 45 days.[19] However, in some sectors the original deadlines were to be kept, whenever possible. 17 18 19

The coronavirus website

An official website has been established for sharing information about the coronavirus.[20] The website provides information and updates to Hungarian citizens concerning news, restrictions, guidance, contact information, hotlines, and global, national, and regional statistics (etc.). The website also lists the deceased, together with information about their age, gender, and chronic diseases (if any).[21] As the list was established at an early stage of the epidemic (March 31, 2020), when the number of deceased was low, identification of the deceased in certain cases was possible, harming the right of reverence.[22] 20 21 22

Surveillance of the quarantined

In light of these actions, the quarantine software deployed in Hungary has to be mentioned. Hungarian citizens, arriving to the country from abroad via passenger traffic, had to undergo epidemiological surveillance and place themselves in quarantine for 14 days.[23] The supervision thereof was the responsibility of the police.[24] On May 4, 2020 the 181/2020 Government Decree made it possible to perform this supervision not only in person but also through software. Based on the consent of the person in self-quarantine, adherence to the respective rules could be supervised through the tracing of their movement, as well as through the processing of their facial image and provided health data. Consent to the installation and use of the software was 23, 24

voluntary,[25] and was informed.[26] However, once consent was provided, the installation and use of the software became mandatory and the omission of its use constituted a misdemeanour. Revocation of consent was possible and the software could be deleted, restoring the general rules of supervision (i.e. regular visits by the police).[27] To enable efficient supervision, the police and the epidemiological authority were entitled to process location data, the facial image of the user, natural personally identifiable data, contact information, and any health data, in connection with the coronavirus. On expiration of the self-quarantine period after 14 days, the user was able to delete the application and the police concluded the supervision, but the data processed throughout the period in question could be processed for another 60 days, unless ordered otherwise by the epidemiological authority or the police.[28]

Such measures deprived citizens from practising their rights. Regardless of the fight against the coronavirus, there were no signs that the effects of the state of danger will necessarily end in Hungary with the end of the epidemic, or guarantees that the processing of the—potentially large amount of—personal data collected will stop. Hungarians live in a country in which they are entirely transparent to the state, not allowed to know essential information about it, and are unable to affect it through their representatives in the National Assembly.[29] Moreover there are threats to those who express their opinions.[30] In conclusion, the government's fight against the coronavirus in Hungary was not only a means to protect citizens—but also to gain further political advantage.

References

1. We follow here the Hungarian Ministry of Justice's choice of language, of a 'state of danger'. A 'state of emergency, along with four further types of special emergency power,' is also mentioned in the Hungarian constitution, but as something other than a state of danger (article 50).

2. See: https://njt.hu/translated/doc/TheFundamentalLawofHungary_20191213_FIN.pdf

3. See: http://njt.hu/translated/doc/J2020R0040K_20200326_FIN.pdf

4. Such empowerment is reasonable considering the need for governing and the potential difficulties to convene the National Assembly.

5. Since 2010, in three consecutive parliamentary elections Orbán's political party, FIDESZ (in coalition with KDNP), has gained a two-thirds majority, allowing them to adopt laws without the need to conduct substantive discussions in the parliament.

6. Enshrined in Articles 8 and 10 of the European Convention on Human Rights, see: https://www.echr.coe.int/Documents/Convention_ENG.pdf

7. Article 3 (1) of Act XII of 2020, see: https://berlin.mfa.gov.hu/assets/77/49/43/cc3672166e33b2cf015ce4371aeedf19417c2710.pdf

8. Article 8 Act XII of 2020.

9. The act LVIII of 2020 on transitional provisions related to the termination of the state of danger was also adopted by Parliament. Although formally the state of danger ended, the abuse of powers is expected to continue. See: https://www.helsinki.hu/en/never-ending-story

10. See: https://magyarkozlony.hu/dokumentumok/c4210b08dd73832b3ca261193f85d508498c9718/megtekintes

11. See: https://magyarkozlony.hu/dokumentumok/13285bbde75a626ff044ec795e70a6ee5d700b29/megtekintes

12. The goal of the information request was to detect, learn about, and prevent the spread of the coronavirus, as well as to organise the harmonised functioning of public bodies. See: https://magyarkozlony.hu/dokumentumok/0862cb1d20ebfb25b36e95142f4e5f28ece35e6a/megtekintes

13. Article 3 (2) 93/2020 (6 April 2020) Government Decree.

14. See: http://njt.hu/translated/doc/J2011T0112P_20190426_FIN.pdf

15. Enshrined in Article 14 of the Privacy Act and Articles 15-22 of the GDPR.

16. See: https://magyarkozlony.hu/dokumentumok/008772a9660e8ff51e7dd1f3d39ec056853ab26c/megtekintes

17. Article 10 (2) Act XII of 2020

18. According to Article 3 (6) of the Privacy Act 'data accessible on public interest grounds means any data, other than data of public interest, the disclosure, availability or accessibility of which is prescribed by an Act for the benefit of the general public.'

19. Extension is possible in case the fulfilment of the request would threaten the fulfilment of public duties of the organ in connection with the state of danger. See Article 2(3) 179/2020 (4 May 2020) Government Decree.

20. See: https://koronavirus.gov.hu

21. See: https://koronavirus.gov.hu/elhunytak

22. See: https://tasz.hu/cikkek/jogserto-listat-kozolt-az-allam-a-koronavirus-aldozatairol

23. See: https://magyarkozlony.hu/dokumentumok/efaa9b4a31e05b8962181d12e2116d1bf71177df/megtekintes

24. Article 3 (1) cb) 81/2020 (1 April 2020) Government Decree.

25. See: https://magyarkozlony.hu/dokumentumok/008772a9660e8ff51e7dd1f3d39ec056853ab26c/megtekintes

26. Article 1 (4) 181/2020 (4 May 2020) Government Decree.

27. For more information about the development and functioning of the software, see: https://index.hu/techtud/2020/06/03/koronavirus_jarvany_hazi_karanten_rendszer_hkr_app_alkalmazas_asura

28. Article 3 (5) 181/2020 (4 May 2020) Government Decree.

29. See: http://www.ekint.org/az-allam-atlathatosaga-informacioszabadsag/2020-05-12/uvegemberkent-elni-a-nagy-testver-orszagaban-avagy-a-lemeszarolt-informacios-szabadsagok

30. See: https://insighthungary.444.hu/2020/05/12/he-criticized-the-government-on-facebook-and-was-taken-from-his-home-by-police-at-dawn

István Böröcz, LLM is a researcher at the research group on Law, Science, Technology & Society at Vrije Universiteit Brussel.

IRELAND

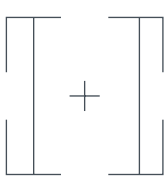
A MARGINAL CONTRIBUTION

TO THE PANDEMIC RESPONSE?

Rob Kitchin

The coronavirus pandemic has posed enormous challenges for governments seeking to delay, contain, and mitigate its effects. Along with measures within health services, and public health measures such as social distancing, self-isolation, quarantining, and lockdowns, a number of countries have sought to implement a range of digital technologies solutions—including smartphone apps, facial recognition and thermal cameras, biometric wearables, smart helmets, drones, and predictive analytics—to limit the spread of COVID-19.[1] 1

The Irish government is presently developing a combined contact tracing and symptom tracking app. In this short essay, I outline the Irish approach to developing this app, initially named CovidTracker Ireland. At least two other similar apps have been developed in Ireland: a contact-tracing app, Tracing Ireland's Population (TIP), produced by private enterprise,[2] and a symptom tracking app, MyCovidSymptons, developed by university researchers and a data start-up.[3] Neither has been endorsed by the government and will likely wither on the vine. In addition, there have been calls for other tech-led solutions to enable a lifting of restrictions, such as the trade union SIPTU's call for temperature testing of workers before accessing meat and food processing plants.[4] 2 3 4



It should be noted that there are dozens of other tech-led initiatives being pursued in order to tackle COVID-19, mostly focused on health services. These initiatives are being actively promoted and supported by the Irish state. For example, the Health Research Board and Irish Research Council launched a rapid-response research call for proposals to deliver medical countermeasures, health service readiness, and social and political countermeasures; and Science Foundation Ireland, Enterprise Ireland, and IDA Ireland are running a scheme to fund research and innovation activities that will help tackle COVID-19.[5] Enterprise Ireland notes that more than 100 client companies are responding to the COVID-19 crisis, and a story in the *Irish Times* reports that Ireland 'ranked in sixth place in a global listing of countries that are responding best to the COVID-19 crisis with innovative solutions.'[6]

CovidTracker Ireland

On March 29, 2020 the Health Services Executive (HSE) announced that it hoped to launch a COVID-19 contact-tracing app within a matter of days. Few details were given about its proposed functionality or architecture,[7] other than it would be opt-in rather than compulsory, respect privacy and GDPR, and be time limited.[8] It was not stated who would develop the app beyond it being described as a 'cross-government effort.'[9] On April 10, the HSE revealed more details through a response to questions from Broadsheet.ie, stating that the now-named CovidTracker Ireland App[10] will help the health service with its efforts in contact tracing for people who are confirmed cases; allow a user to record how well they are feeling, or track their symptoms every day; provide links to advice if the user has symptoms or is feeling unwell; and give the user up-to-date information about the virus in Ireland.

There was no mention of the approach being taken; however, the presence of the HSE logo on the PEPP-PT (Pan-European Privacy-Preserving Proximity Tracing) website[11] indicated that it had adopted that architecture;[12] an architecture that was being used by seven countries in Europe at the time.[13]

From the date of its announcement, concerns were expressed about the CovidTracker Ireland, particularly by representatives of Digital Rights Ireland and the Irish Council for Civil Liberties. A key issue was the lack of transparency and openness in the approach being taken. There were also concerns that a centralised, rather than decentralised approach to data collection was being taken, and there was no sense that the underlying code would be open for scrutiny.[14] There were no details about where data would be stored, who would have access to it, how it would be distributed and acted upon,[15] and there was unease as to whether the app would be fully compliant with GDPR, and whether a Data Protection Impact Assessment (DPIA) would be published in advance of its launch.[16] In addition, critics were concerned that CovidTracker Ireland merged the tasks of contact tracing and symptom tracking—given that the latter records personal information, and is not required to perform the former. They were worried that CovidTracker Ireland might become a 'super app', enabling control creep with respect to quarantine enforcement and movement permission,[17] or that it might become 'mandatory but not compulsory for people who deal with the public or work in a shared space.'[18]

14
15
16
17
18

By late April, there had been a number of newspaper articles, blog posts, and radio interviews questioning the approach being taken and the prospective utility and effects of the app. The Irish Council of Civil Liberties, Digital Rights Ireland, and a number of academics wrote an open letter to the government demanding that there be much more transparency in the process and that the government follow all the recommendations of the European Data Protection Board.[19] With pressure mounting, more details about the app started to leak to the media, including confirmation that a centralised approach had been pursued,[20] that it would combine contact tracing and symptom tracking, and that the app was being developed by Nearform, an Irish tech company.[21] This pressure led to a fundamental shift in the approach at the close of the month, with the app swapping from a centralised to a decentralised approach to data collection, following the lead of most European countries. On April 30, the Health Minister was questioned on the app in the

19
20
21

Dáil (Irish parliament), and on May 2, a statement and briefing on the app was published.[22] While providing some information, the demands for details on the draft specification and user requirements, DPIA, and source code remain unanswered.

Testing took place in early June, and the DPIA and source code was released in the last week of June and was generally praised by commenters, though there remains concerns over efficacy, proportionality and necessity.[23] The launch of the app is expected to take place in the first part of July. The app will work independently of the app in Northern Ireland, which might cause some issue given the open border between the jurisdictions. It would be nice to think that the CovidTracker Ireland app will make a difference to containing COVID-19 and help halt any additional waves of infection. However, this seems unlikely given that it is unlikely to be adopted at sufficient scale to be effective, given widely held concerns with respect to its development and use. Any move to make the use of the app mandatory to ease lockdown restrictions or gain access to work or public space will be met with resistance from civil liberties groups and the general population. Furthermore, the symptom tracking relies on self-reporting, which lacks rigour, and as testing has shown, a large proportion of the population has tested negative for COVID-19, despite showing symptoms—potentially leading to a large number of false positives. As such, the app seems set to make only a marginal contribution to how Ireland deals with the COVID-19 crisis.

References

1. Kitchin, R. (2020) Civil liberties or public health, or civil liberties and public health? Using surveillance technologies to tackle the spread of COVID-19, *Space and Polity*, DOI: https://doi.org/10.1080/13562576.2020.1770587
2. See: https://www.irishexaminer.com/breakingnews/ireland/limerick-brothers-design-new-contact-tracing-app-993694.html
3. See: https://www.siliconrepublic.com/innovation/covid-19-symptom-tracker-ireland-data
4. See: https://www.rte.ie/news/2020/0501/1135981-covid-19-cases-plant
5. See: https://www.irishtimes.com/news/science/urgent-call-out-for-irish-scientists-to-help-global-coronavirus-response-1.4217710

6. See: https://www.irishtimes.com/business/innovation/ireland-ranked-among-best-for-covid-19-innovative-solutions-1.4233471

7. See: https://www.siliconrepublic.com/enterprise/hse-coronavirus-contact-tracing-app ; https://www.irishtimes.com/business/technology/coronavirus-contact-tracing-app-raises-privacy-concerns-1.4219224

8. See: https://www.siliconrepublic.com/enterprise/hse-coronavirus-contact-tracing-app ; https://www.irishtimes.com/business/technology/coronavirus-contact-tracing-app-raises-privacy-concerns-1.4219224 ; https://www.irishtimes.com/news/ireland/irish-news/coronavirus-privacy-advocates-say-hse-planning-a-super-app-1.4225992

9. See: https://www.siliconrepublic.com/enterprise/hse-coronavirus-contact-tracing-app

10. See: https://www.broadsheet.ie/2020/04/10/covidtracker-ireland-app-and-you

11. https://www.pepp-pt.org

12. See: https://twitter.com/CBridge_Chief/status/1251521163668475905

13. See: https://techcrunch.com/2020/04/17/europes-pepp-pt-covid-19-contacts-tracing-standard-push-could-be-squaring-up-for-a-fight-with-apple-and-google

14. See: https://www.irishtimes.com/business/technology/coronavirus-contact-tracing-app-raises-privacy-concerns-1.4219224 ; https://thegist.substack.com/p/the-gist-whats-with-the-covid-apps

15. See: https://thegist.substack.com/p/the-gist-whats-with-the-covid-apps

16. See: https://www.irishtimes.com/business/technology/coronavirus-contact-tracing-app-raises-privacy-concerns-1.4219224 ; https://thegist.substack.com/p/the-gist-whats-with-the-covid-apps

17. See: https://www.irishtimes.com/news/ireland/irish-news/coronavirus-privacy-advocates-say-hse-planning-a-super-app-1.4225992

18. See: https://www.irishtimes.com/news/ireland/irish-news/coronavirus-privacy-advocates-say-hse-planning-a-super-app-1.4225992

19. See: https://www.iccl.ie/news/hse-app-experts-and-public-need-to-see-details

20. See: https://www.irishtimes.com/business/technology/hse-covid-19-tracing-app-data-will-be-stored-on-individual-devices-1.4240304

21. See: https://www.irishtimes.com/business/technology/the-frontline-of-the-fight-against-covid-there-s-an-app-for-that-1.4235094

22. See: https://www.gov.ie/en/news/d2a00d-national-app-for-covid-19

23. See: https://www.irishtimes.com/news/ireland/irish-news/hse-reveals-key-documents-ahead-of-covid-19-tracker-app-1.4289700

Rob Kitchin is a professor at Maynooth University, Ireland. His most recent book is 'Slow Computing: Why We Need Balanced Digital Lives' (Bristol University Press).


JAPAN
HIGH
AND
LOW TECH

RESPONSES

David Murakami Wood

Before the app

Before April 15, 2020, the day on which the Japanese government announced the development of a contact-tracing app, Japan had not showcased any novel technologies of pandemic containment or monitoring.[1] Given that the government is advancing a highly future-oriented series of policies towards 'Society 5.0',[2] this lack of innovation in response to COVID-19 is surprising.

The response to the challenge of COVID-19 in Japan has largely been low-tech. While the use of both dashboard-style websites[3] and the pervasive Line social media system, by national and local governments, has been significant for distributing information to the public, data gathering and collation in large companies, government departments, and especially local governments, is often still carried out with pencils, paper, fax machine, and inked stamps (*hanko*), and there has been no change in these practices in response to the pandemic. Fax machines have remained central to Japanese bureaucracy since Japan became the global leader in their use in the late 1980s and remained so long after other countries had abandoned fax for email.[4] Mistakes in counting the numbers of infected in Tokyo has been attributed to overworked public health employees 're-copying what had been entered into the terminal by hand (and then faxed).'[5] This bureaucratic-technological path-dependency has also resulted in 80% of office workers claiming to have had no choice but to go into work physically because they had to use official corporate *hanko*.[6]

One of the basic problems in assessing Japan's response has been the lack of reliable data. Japan's official figures look very good compared to other comparable countries. However, until

recently raw data was unavailable, which led to a suspicion that the real numbers were being hidden. The government contested this, arguing that the death rates were broadly correct, because 'Japan conducts surveillance for pneumonia, so almost all cases of pneumonia undergo a CT scan, and most
7 of those would do a PCR [Polymerase Chain Reaction] test'.[7] The Tokyo Metropolitan Government has now released full COVID-19 infection and mortality figures for the first quarter of 2020. The mortality rates do not indicate a rise in unexplained
8 deaths.[8] But suspicions persisted, not least because the figures themselves reflect a very low testing rate, particularly compared to neighbouring South Korea and Taiwan. Finally, in late May, the National Institute for Infectious Diseases released an analysis for Tokyo for the five weeks from February 17 that showed that there was an order of magnitude difference between the official deaths from COVID-19 and the excess mortality in the city over this period: 16 people had officially died as a result of the pandemic but there were over 50-60 further excess deaths per week during that time, or 250-300
9 in total.[9] This was attributed to a combination of slow reporting processes, which again had to do with the technologies involved, and the lack of PCR testing.

The Abe government discouraged PCR testing for the virus for individual diagnosis and data collection by local governments on the grounds that it would overwhelm them. According to the activist Shigeru Wakita, neoliberalisation and deep cuts made progressively over the last 25 years to local (and national) public health budgets have contributed to
10 the pandemic response.[10]

The surveillance studies scholar and activist Toshimaru Ogura has expanded on this thesis, arguing that not only are neoliberalising cuts to local public services to blame but also, since 9/11, an increasing (re)militarisation of pandemic emergency responses, with a shift away from simply disaster and disease to 'natural disasters, pandemics of infectious diseases, and terrorism.' In the preparations for the 2020 Olympic and Paralympic Games, this shift in
11 emphasis towards terrorism became even more evident.[11]

The lack of preparedness and cuts in local funding, which has meant a shortage of accessible critical care beds, has had tragic consequences during this pandemic. Social media has seen many personal stories of people unable to find a hospital bed, with some of these gaining media attention.

One reason why publication of low infection figures would be desirable was due to government concerns that the 2020 Tokyo Olympic Games would be postponed or cancelled. Until Japan was eventually forced to postpone by the International Olympic Committee in March, under pressure from athletic organisations worldwide, there were persistent accusations from senior doctors like Shinji Shimada, the President of Yamanashi University,[12] that the state was deliberately making it as hard as possible to obtain a PCR test, suppressing infection data, encouraging doctors to diagnose possible COVID-19 cases by the secondary conditions generated, and even misrecording the cause of death as being by these conditions. However, the government has contested this, arguing that their approach to PCR testing was deliberately designed for cluster tracing not individual diagnosis.[13]

12

13

Political analysis may not then explain Japan's infection and death rates, which even accounting for manipulation remain low by global standards. An alternative, or additional explanation, is the cultural hypothesis, which posits that Japanese society has several traits that makes infectious disease spread less rapidly and widely, notably:

> (1) A propensity towards distance and reserve. Japanese people do not generally touch each other in public and especially not skin-to-skin.
> (2) Everyday hygiene. Hand-washing is frequent, taking off shoes before entering houses is normal, etc.
> (3) Responsibility for disease prevention. Wearing non-medical face masks is normal for anyone with disease symptoms, to protect others.

The cultural hypothesis is hardly a new observation, but is often dismissed by observers who seek more specific, clearly measurable reasons for Japan's seemingly inexplicable success in confronting the COVID-19 pandemic, when the answer appears to be more holistic and indeed cultural. The face mask in many ways may be the most important and emblematic technology deployed in Japan to fight COVID-19. As Wada and colleagues concluded in their assessment of the efficacy of mask-wearing in relation to the annual influenza season in Japan:

> 'wearing a face mask in public may be associated with other personal hygiene practices and health behaviors among Japanese adults. Rather than preventing influenza itself, face mask use might instead be a marker of additional, positive hygiene practices and other favorable health behaviors in the same individuals.'[14]

However, cultural factors have not all been positive. There have been reports of widespread exclusion and bullying of those with, or suspected of being infected with, COVID-19, and even of healthcare workers, in a complete reversal of the celebratory attitude observed in most other countries.[15]

In addition, while Japanese people have a reputation for social compliance connected to responsibilisation, the broadly voluntary measures to control movement, encourage people to work from home, and avoid entertainment centres, have not been universally observed. Government advice not to gather in crowds was also undermined by the fact that metro and train lines, the places where people are most likely to be packed together, were not closed down or even restricted.[16]

Contact-tracing apps

On April 15, 2020, a press release from a national 'civic hacking' organisation called Code for Japan[17] announced the development of a contact-tracing app for Japan, which had in fact been in development since late March.[18] Not much detail was provided, however three important aspects were visible

even at this stage: (1) that the model was 'the one developed by GovTech Team in Singapore'; (2) that the app would be tightly restricted in its function, would not be universal, and would protect privacy because 'the user and the infected contact person are *not* notified when, where, and with whom the contact is made'; and finally (3) that it would 'comply with joint standards of Apple and Google'.[19] The media was slow to pick up on the development, however stories appeared by the end of the month in which the app was now described as a government app, developed *with* Code for Japan.[20] However, it was not until the second week of May that more detail was made available.

19

20

In the meantime, significant critiques had started to appear, notably a five-part series in the Asahi Shimbun, an influential national newspaper, which considered the development and use of contact-tracing apps, pointed out some of the problems with them, and reminded readers of the ways in which Japan was bound up in both military and capitalist networks with the US—networks which include the very companies which created the protocols underlying Japan's app.[21]

21

By May 8, 'the government decided that the Ministry of Health, Labor and Welfare will take the lead in the development of a new coronavirus infection tracking app that was being promoted jointly by the public and private sectors'.[22] Code for Japan was credited as the developer, but now in conjunction with the Rakuten corporation, and it was emphasised once again that the system would be based on the Apple–Google protocols, that it would use only anonymised data, and would not track the user outside of actual moments of localised (Bluetooth) contact between users of the app.

22

By the next week the app had an official name—'Mamoriai' ('Protecting Together')—and the developers began to post more details.[23] This in itself is interesting in the Japanese governmental context, in which government departments are generally highly opaque and consultation is something to be avoided. One of the UX/UI designers reflected openly on the difficulties of balancing clarity and ambiguity in an app that cannot offer certainty about whether someone is actually

23

infected; but they also argued that the Mamoriai team was doing as much as they could for privacy, describing the app explicitly for the first time as decentralised.[24]

Hal Seki, the director of Code For Japan, added that 'We will also publish all of our source code and specifications [...] We plan to open source it, but we will report it on this blog etc. as soon as the schedule is decided.' However, this apparently smooth progress was suddenly disrupted in early June, when the government released not Code for Japan's app, but a completely different one called 'Cocoa'—also based on the Apple–Google API, and apparently developed by a much more secretive team of Microsoft engineers[25] and subcontracted to a private sector IT consultancy, Persol.[26]

It may well be that contact-tracing apps are intrinsically flawed as a strategy for many reasons—even the creators of the Bluetooth technology on which they depend have questioned whether it is capable of what is being promised.[27] However, it is generally acknowledged that if an app is to be used, then a limited, anonymised, decentralised, open source app would be the most privacy-respecting solution. However, this is not to say there is no risk attached, given that 'any decentralised scheme can be turned into a centralised scheme by forcing the phone to report to the authorities that it was at some point in time close to the phone of an infected person.'[28] And in addition, new questions must now be asked about the process of app development, how decisions were made, and who will benefit from those decisions.

Japan is now lifting its state of emergency, and this may turn out well or badly. But either way, as several commentators have argued, Japan has done well despite (and not as a result of) Abe's strategy.[29] It remains to be seen whether the Cocoa app will be deployed successfully, whether it will be used to any great extent, and whether it does indeed form the basis for an extension of other forms of state surveillance.

References

1. For more on the issues in this dispatch, see: Murakami Wood (2020). Apps, Face Masks and Fax Machines: Japan, Technology and COVID-19. Unpublished paper, available from the author.

2. See: https://www.alt-movements.org/no_more_capitalism/blog/2019/07/04/society50hihan

3. See e.g. the Tokyo Metropolitan Government's dedicated COVID-19 website: https://stopcovid19.metro.tokyo.lg.jp

4. Coopersmith, J. (2015) *Faxed: The Rise and Fall of the Fax Machine.* JHU Press.

5. See: https://www3.nhk.or.jp/nhkworld/en/news/backstories/1088

6. See Note 5 above.

7. According to Shigeru Omi, deputy head of the government's advisory panel on the virus. See: https://asia.nikkei.com/Spotlight/Coronavirus/Coronavirus-Why-Japan-tested-so-few-people

8. See: https://www.japantimes.co.jp/news/2020/05/09/national/tokyo-releases-covid-19-data

9. See: https://asia.nikkei.com/Spotlight/Coronavirus/Tokyo-s-excess-deaths-far-higher-than-COVID-19-count-data-shows

10. All translations done using Google Translate and corrected by the author. See https://hatarakikata.net/11189

11. See: https://www.alt-movements.org/no_more_capitalism/blog/2020/04/23/cyclical-pandemic

12. See: https://toyokeizai.net/articles/-/349413

13. See: https://asia.nikkei.com/Spotlight/Coronavirus/Coronavirus-Why-Japan-tested-so-few-people

14. See: https://doi.org/10.1186/1471-2458-12-1065

15. See: http://www.asahi.com/ajw/articles/13362712

16. See: https://foreignpolicy.com/2020/05/14/japan-coronavirus-pandemic-lockdown-testing

17. Code for Japan, see: https://www.code4japan.org

18. See: https://note.com/hal_sk/n/n0e05f3482d28

19. See: https://prtimes.jp/main/html/rd/p/000000008.000039198.html

20. See: https://english.kyodonews.net/news/2020/04/7fc1fa19ec2d-japan-govt-to-release-coronavirus-contact-tracing-app-in-may.html

21. See: https://globe.asahi.com/

article/13331044 ; https://globe.asahi.com/article/13351680 ; and https://globe.asahi.com/article/13370568

22. See: https://www.asahi.com/articles/ASN5D5VLHN58ULFA01Y.html

23. See: https://note.com/hal_sk/n/n0e05f3482d28 ; https://note.com/shosira/n/nccb92bf21913

24. See: https://note.com/shosira/n/nccb92bf21913

25. See: https://asia.nikkei.com/Spotlight/Coronavirus/Contact-tracing-app-set-to-debut-in-Japan-this-week

26. See: https://xtech.nikkei.com/atcl/nxt/news/18/08122

27. See: https://theintercept.com/2020/05/05/coronavirus-bluetooth-contact-tracing

28. See: https://blog.xot.nl/2020/04/11/stop-the-apple-and-google-contact-tracing-platform-or-be-ready-to-ditch-your-smartphone

29. See: https://asia.nikkei.com/Opinion/Japan-s-coronavirus-response-is-flawed-but-it-works ; https://foreignpolicy.com/2020/05/14/japan-coronavirus-pandemic-lockdown-testing

David Murakami Wood is Associate Professor in Sociology and member of the Surveillance Studies Centre at Queens's University, Ontario.


JORDAN
AN
E-GOVERNMENT
STRATEGY

THAT OVERLOOKS DIGITAL DIVIDES

Raya Sharbain and Anonymous II

On March 17, 2020, in a rush to contain the spread of the COVID-19 virus, Jordan's government activated the 1992 Defence Law.[1] Almost immediately, land borders, the international airport, and schools were closed, nearly all economic activity halted, and the government imposed a three-day total lockdown, followed by a strict daily curfew that only started to relax on June 6, but remains in place for late evenings at the time of writing. Up until late April, people could not use cars—the main mode of transportation in Jordan—without a special permit and once the strict lockdown was lifted, people were only allowed to walk to local supermarkets for provisions.

1

Since announcing the lockdowns and subsequent curfews, Prime Minister Razzaz's government has relied much more heavily on digital platforms like the Web and mobile applications to ease the burdens imposed by coronavirus containment efforts, and to assist the country with the gradual reopening of different sectors. In readiness for the surge of Internet usage, the Telecommunications' Regulatory Commission (TRC) expanded network providers' capacities
2, 3 in March.[2] Arguably, the release of multiple digital platforms[3] represents what we might call the digitisation of the social compact between citizens and the government.

Jordan's digital divide

In some ways, this techno-solutionist approach to government service delivery has laid bare the stark digital inequalities that exist in the country, and the government's slow response to mitigate the divide brought about by its digital strategy. With the urgent jump to remote learning, the government rushed to develop an online courses platform, a learning management system, a teachers' skills platform, and an e-textbook repository, praising local private sector support in the development of all these systems. While the speed with which these platforms were developed was unprecedented, it did not pay attention to unequal Internet and device access
4 amongst students in Jordan.[4] The World Bank estimates that while 84% of students have Internet access for remote learning, only two-thirds have a computer they can use for schoolwork—below the
5 MENA average of 75%.[5] The government started taking action two months into the
172 shutdown, just as school semesters were drawing to a close, distributing donated
6 tablets (mostly from Huawei),[6] and building caravans equipped with computers, televisions, and satellites in remote governorates such as
7 Tafilah.[7] This has led to vulnerable communities receiving
8 a poorer quality education during the pandemic.[8]

To help facilitate salary transfers, ensure safer alternatives to cash payments, and monitor labour law violations, the government has started pushing the use of Central Bank of
9 Jordan approved e-wallets,[9] even though polls have shown

that more than half of users find them difficult to create and use.[10] Furthermore, these e-wallet platforms are being introduced in the absence of strong privacy protection laws, and it is unclear how user privacy is being protected.

The drive to digitisation has made people in Jordan vulnerable to a range of digital security challenges.[11] For instance, opportunists took advantage of the government's rush to digital platforms to launch official-looking phishing scams targeting unsuspecting users,[12] a situation which speaks to the challenges of digital literacy.

The rise of monitoring tech

Jordan's Defence Law No. 13 (of 1992), activated by royal decree at the start of the shutdown,[13] gives the government broad authority to issue orders under the law and curb basic rights. Yet while Prime Minister Razzaz implied that the government would not infringe on basic rights and that the law 'will be used within the tightest limits',[14] he also indicated that distinctions would 'be made between the right to express an opinion, which is inviolable, and defamation, spreading rumours, and false information that could cause panic. We will deal with [the latter] firmly.'[15] Since then, journalists have been detained for reporting on the plight of Jordanians as well as migrant workers in the country during the lockdown.[16] And then in mid-April, the government introduced Order Number 8 which targets online 'scaremongering', punishable with up to a three-year prison sentence and fines up to 3,000 JOD (around US$4,300/EUR3,800), thus empowering the government's online watchdog.[17]

Under the Defence Law, there has been a concomitant introduction of monitoring tools, from contact tracing, to reporting social distancing violations, and enforcing home quarantine for those returning from abroad. According to the Minister of Health, Saad Jaber, these applications represent important steps 'in the fight against the virus.'[18] Jaber announced, amongst other applications, a contact-tracing application called Aman, which (at the time of writing) is voluntary to download and use.[19] The application is closed source,[20] yet promises to respect privacy—the privacy policy does indeed state that data is only stored locally and

anonymously. The Ministry has suggested that it is a 'moral and human duty towards others to download and use [the app].'[21] The application says it will log GPS coordinates initially, then transition to only logging Bluetooth transmissions from nearby smartphones. Some have argued the latter is a privacy-promoting move (see DP3T protocol)[22] while critics suggest that such a feature will exhaust older phone models' batteries as they are not equipped with low-energy Bluetooth chips.[23] At the time of writing, the application has over 600,000 downloads,[24] with government officials repeatedly asking people to download the application, and constantly reminding those who have downloaded the application and received notification of proximity to an infected person to visit the nearest COVID-19 dedicated health centre.[25]

The application CRadar was also launched, which allows people to report large gatherings and when they suspect someone has symptoms of COVID-19.[26] They do so by sharing the location of the incident / person with the authorities via the application. This approach has been criticised for encouraging people to report on each other, though it remained in use mostly during strict curfew.

For Jordanians returning from abroad, once they complete the 17-day mandatory quarantine in government facilities, the government mandates the use of an application called Bader during their 14-day home quarantine.[27] There are reports that suggest that the application will be accompanied by an electronic bracelet. On Saturday June 20, the Health Minister announced that the bracelets will be worn by people required to home quarantine; the bracelet accompanies the application Bader.[28,29]

These monitoring applications, which vary in purpose and in intention, feed into Jordan's 'panoptic' approach to containing the spread of COVID-19. In combination with a personal data protection bill that is still being debated in parliament (which currently is not in session)—there appear to be few legal provisions for citizens and users beyond the privacy policies (if any) of the applications. The unequal connectivity and access to devices and smartphones, combined with the problems inherent to digital contact

tracing and quarantine enforcement, and the absence of strong data protection laws, means that Jordanians are unable to meaningfully and sustainably benefit from the digitisation of the social compact with their government that has emerged with the COVID-19 pandemic.[30] This may make the longer-term recovery even more challenging.

References

1. See: https://www.hrw.org/news/2020/03/20/jordan-state-emergency-declared
2. See: https://en.royanews.tv/news/20388/Orange-commends-TRC%E2%80%99s-decision-to-offer-higher-bandwidths--assures-readiness-to-provide-best-service
3. See: https://jordantimes.com/news/local/new-website-launched-streamline-access-covid-19-platforms
4. See: https://blogs.ucl.ac.uk/ceid/2020/05/05/batshon-shahzadeh
5. See: https://blogs.worldbank.org/arabvoices/covid-19-and-digital-learning-preparedness-jordan
6. See: https://www.jordantimes.com/news/local/cpf-provides-tablet-devices-students-remote-areas-boost-education-ministry-efforts
7. See: https://bit.ly/3h4gS4q
8. See: https://bit.ly/2DCd8ZA
9. See: https://www.facebook.com/337787836856046/posts/598851197416374
10. See: https://www.jordantimes.com/news/local/e-wallets-are-not-easy-create-pool-finds
11. See: https://www.ammonnews.net/article/533729
12. See: https://www.facebook.com/MoDEEJO/photos/a.10151674158922676/10156783642942676
13. See: https://kingabdullah.jo/en/news/royal-decree-approves-cabinet-decision-proclaim-defence-law
14. See: https://twitter.com/PrimeMinistry/status/1239977527382290433
15. See: https://twitter.com/PrimeMinistry/status/1239977492502523904

16. See: https://www.hrw.org/news/2020/05/06/jordan-free-speech-threats-under-covid-19-response
17. See: https://bit.ly/2WoiT3A
18. See: https://twitter.com/PrimeMinistry/status/1263529565642797060
19. See: https://www.amanapp.jo/ar
20. See: http://opinions.jordanopensource.org/post/250
21. See: https://bit.ly/30j2ChQ
22. See: https://github.com/DP-3T
23. See: https://arstechnica.com/tech-policy/2020/04/2-billion-phones-cannot-use-google-and-apple-contract-tracing-tech
24. See: https://bit.ly/2WnIlpo
25. See: https://bit.ly/30fu5k7
26. See: https://bit.ly/3fIY6jb
27. See: https://bit.ly/2ZvPO8q
28. See: https://youtu.be/R5X3fDoC00A?t=1418
29. See: https://twitter.com/PrimeMinistry/status/1274362121359417344
30. See: https://ali-alkhatib.com/blog/digital-contact-tracing

Raya Sharbain is a programme coordinator at the Jordan Open Source Association in Amman, Jordan. She has written on matters of digital rights in Jordan.


KENYA
PLACING
ALL
THE BETS

ON HIGH TECHNOLOGY TECHNOLOGY

Grace Mutung'u

Kenya prides itself amongst Africa's technology hubs and was, even prior to the COVID-19 pandemic, in the process of implementing several large-scale digitisation projects. Since the announcement of its first official case on Friday March 13, technology has been featured as a solution for access to information, education, finance, justice, and public order. The national broadcaster and many private education providers have been delivering broadcasts for children following school closures. The Central Bank has also given directives on cost-free mobile money transfers to encourage cashless transactions. The judiciary has embraced electronic case management and has published practice directions that guide management of civil cases.[1] And the president has announced a partnership with Google Loon for provision of Internet services to underserved areas to support home working.[2] On April 21, the ICT Cabinet Secretary appointed an ICT Advisory Committee to 'coordinate ICT specific responses' to the pandemic.[3] Most of these ICT proposals are proposals for mobile tracing apps.

1

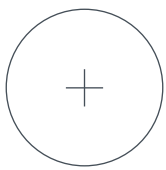
2

3

Not all of Kenya's pandemic policy responses are published, and following the narrative of using technology to fight the unseen enemy, the security services have advanced their surveillance practices, almost unnoticed. Before the suspension of air travel, the Ministry of Health began to

collect telephone contacts of those entering the country and
4 monitor if they were following self-quarantine directives.[4]
Public service vehicles (matatu) were also instructed to
register phone numbers and national ID numbers of their
passengers and to use cashless means of collecting fares.
These measures have since been abandoned as they proved
5 impractical for short distance trips.[5]

During the initial days of the pandemic, neighbourhoods
were treated to dramatic visits by health surveillance teams
who collected information, disinfected dwellings, and ferried
6 suspected patients about in ambulances.[6] Contact tracing
has been less visible, as it is undertaken by the national
intelligence service who were allocated Ksh. 1.5 billion (about
15m USD), in the latest emergency budget to boost their
7 case and contact-tracing operations.[7] The tracing is done in
conjunction with mobile network operators
who help triangulate the contact's phone
number to the nearest cell phone masts
180 to determine their location. Information
such as other phone users with whom they
might have been in physical proximity is
8 then inferred from these data.[8]



Digital surveillance is not limited to contact tracing. It is also
used in monitoring of social media for misinformation. A
staffer at the national airline who shared footage of a plane
landing from China after the government had halted flights to
9 China was quickly suspended.[9] The government has warned
the public against sharing fake information about the virus,
and forwarded any concerned accounts to law enforcement
10 for investigation.[10] At least four people have been arrested
11 for sharing false information.[11]

Despite knowing that social media are monitored, Kenyans
are still online, organising and responding to challenges
brought about by the pandemic. They have used the same
social media to raise awareness of police brutality during the
12 curfew,[12] call out leaders not adhering to Ministry of Health
guidelines, and to organise mutual aid for those in need.
Locals have created simple inventions such as handwashing
13, 14 jerricans[13] and masks made from leftover fabric[14] as they

waited for interventions from the government bureaucracy,[15] which was in turn awaiting loans from development partners.[16] With hindsight from previous health emergencies such as HIV/AIDS, community-based care is already proving to be useful in managing COVID-19 illness and deaths, and as physical distancing is limited, digital tools are handy.

Health surveillance has already helped in apprehending people who have escaped from quarantine and helped to produce maps for decisions such as restriction of movement and mass testing.[17] However, surveillance can be—and in the past has been—an overreach. It is therefore worrying that the nature, actors, and safeguards, if any, of Kenya's digital surveillance remain unclear to the public.

This is not because there is a lacuna in the law. The constitution guarantees privacy, including protection from communication and private and family affairs being revealed unnecessarily. The Data Protection Act, enacted in late 2019, makes it mandatory to register all data processing activities with the office of the Data Protection Commissioner. Unfortunately, the act has not yet been operationalised. There is no Data Protection Commissioner, although the recruitment has begun.

The pandemic comes at an interesting time in digital technology policy making. The Kenyan high court had at the end of January declined to address the impact of technology used in digital ID on human rights.[18] It instead gave the government a green light to roll out the ambitious digital ID programme Huduma Namba (Swahili for service number) on the condition that a legal framework be first put in place. Shortly thereafter, the court also okayed the Computer Misuse and Cybercrimes Act (CIMA), known in digital rights circles as the 'fake news' law.[19] The law not only reintroduces criminal defamation, but has already been put to use in prosecuting speech relating to the pandemic. In a season of go-aheads, the court of appeal in April found that the communications regulator is justified in making a database of all mobile devices in Kenya under a project known as the Device Management System (DMS).[20]

These cases show an increasing acceptance of technology by the courts, contrary to a few years ago where they made more cautious findings that were quite protective of fundamental rights. The DMS project, for example, was halted by the high court in 2018, creating a precedent on
21 privacy that many cases have relied upon.[21] Similarly, criminal defamation was declared unconstitutional in 2017, putting a halt to the practice of arresting and charging bloggers
22 whose content clashed with the political elite.[22] Prior to that, bloggers had been charged under the infamous section 29 of the Kenya Information and Communication Act (KICA) that outlawed 'misuse of a licenced communication system'. It
23 was annulled in 2016.[23]

Although the virus presents a new challenge, digital policing is a familiar practice in Kenya. Every election year, resources are reserved for monitoring online content so as to prevent a recurrence of the post-election violence witnessed in 2008. Monitoring of persons of interest is also applied in the
182 fight against terrorism. In these previous uses, engagement of stakeholders and use of community mechanisms have proved to be important complementary aspects for peace building. Of course, digital technology has its limitations and potential fallibilities. Even in a pandemic, the public should be given an opportunity to understand and interrogate the technological measures being applied for their safety.

References

1. See: http://kenyalaw.org/kl/index.php?id=10211
2. See: https://www.president.go.ke/2020/03/23/kenya-approves-roll-out-of-google-loon-4g-to-mitigate-coronavirus-work-disruptions
3. See: https://ca.go.ke/about-us/who-we-are/ict-advisory-committee-on-covid-19
4. See p. 58: https://kma.co.ke/Documents/Case%20management%20protocol.pdf
5. See: https://www.the-star.co.ke/news/2020-03-17-matatus-weak-link-in-anti-corona-war
6. See: https://www.youtube.com/watch?v=5-Qdx4RX7oQ
7. See: https://www.the-star.co.ke/news/2020-04-22-sh40bn-allocated-to-corona-response-treasury-cs-yatani

8. See: https://www.nation.co.ke/news/How-State-is-tracking-down-virus-rebels/1056-5514640-15c6nypz/index.html

9. See: https://www.nation.co.ke/news/Kenya-Airways-suspends-employee-JKIA-coronavirus-drama/1056-5471904-y1at63/index.html

10. See: https://citizentv.co.ke/news/govt-says-dci-now-investigating-fake-news-alarming-videos-on-coronavirus-326496

11. See: https://www.standardmedia.co.ke/article/2001364432/kenyan-man-arrested-for-fake-corona-virus-post-on-social-media ; https://www.the-star.co.ke/news/2020-03-20-blogger-alai-to-spend-night-in-police-cells-over-covid-19-tweet ; https://www.nation.co.ke/news/Coronavirus-blogger-Nyakundi-in-trouble/1056-5503658-hsrnk0z/index.html

12. See: https://www.aljazeera.com/news/2020/06/protesters-march-kenyan-police-brutality-200608162743597.html

13. See: https://www.youtube.com/watch?v=ZGfZGQyEaqk

14. See: https://www.aljazeera.com/news/2020/04/kenyas-coronavirus-fight-factories-tailors-cloth-masks-200417095635189.html

15. See: https://www.capitalfm.co.ke/news/2020/04/kebs-commits-to-facilitate-tailors-in-the-production-of-standardized-face-masks

16. See: https://www.capitalfm.co.ke/business/2020/05/kenya-receives-sh133-3bn-in-loans-in-just-3-days-after-afdb-lends-govt-sh21-9bn

17. See: https://www.nation.co.ke/news/How-State-is-tracking-down-virus-rebels/1056-5514640-15c6nypz/index.html

18. See para 875: http://kenyalaw.org/caselaw/cases/view/189189

19. See: http://kenyalaw.org/caselaw/cases/view/191276

20. See: http://kenyalaw.org/caselaw/cases/view/193383

21. See: http://kenyalaw.org/caselaw/cases/view/151117

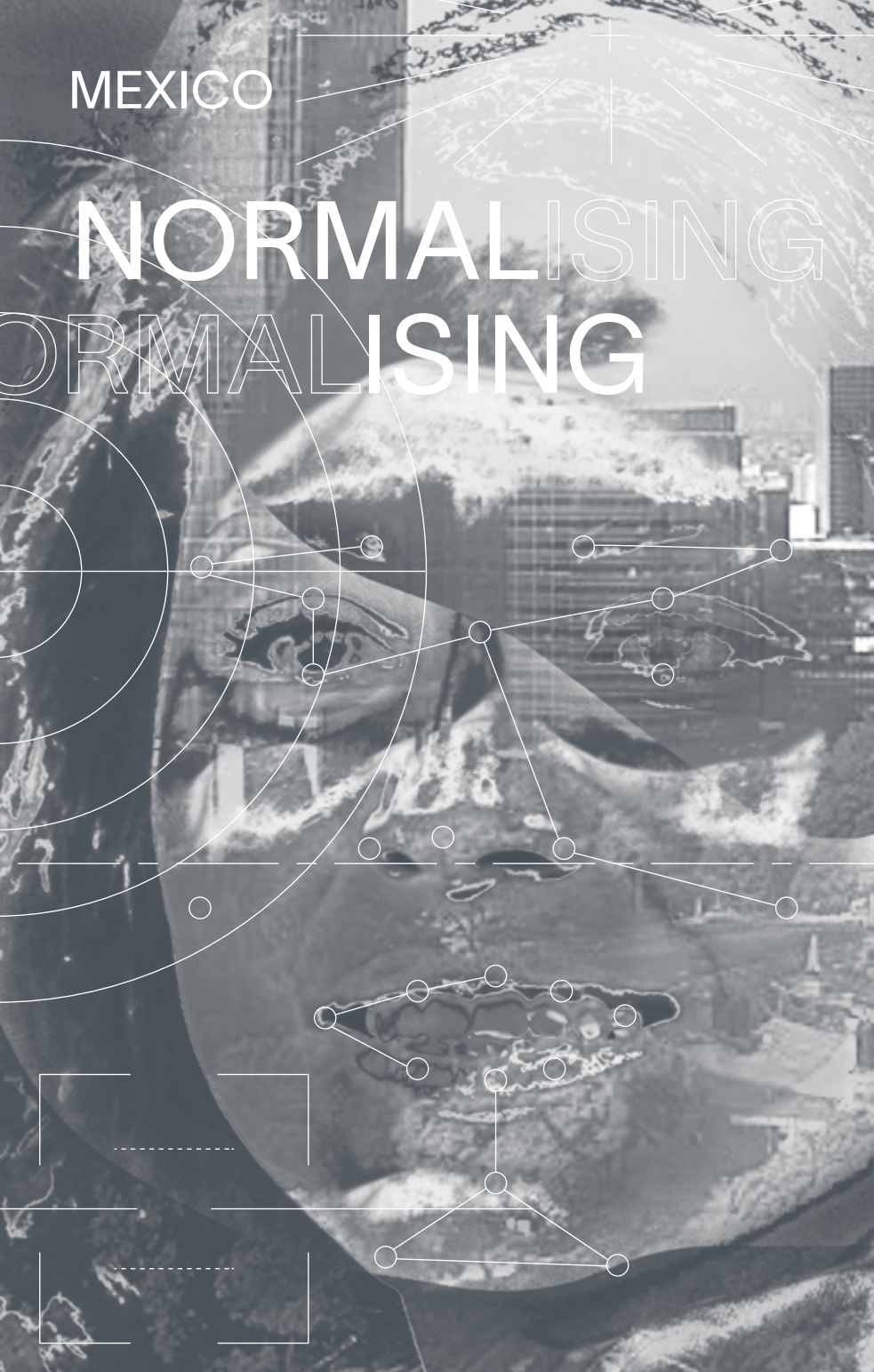
22. See: http://kenyalaw.org/caselaw/cases/view/130781

23. See: http://kenyalaw.org/caselaw/cases/view/121033

Grace Mutung'u is a research fellow at the Centre for IP and IT Law (CIPIT) at Strathmore University, Nairobi.

MEXICO

NORMALISING



DIGITAL SURVEILLANCE

Arely Cruz-Santiago

'Google and Apple can let the Health Secretary know if you are not staying at home', reads the title of a news article, quoting Ricardo Cortés Alcalá, Director General for the Promotion of Health in Mexico, who candidly declared that the Ministry of Health is using location data facilitated by Apple and Google in order to determine population-wide mobility patterns:

> '...if you allowed any mobile app on your phone to use its location service, then you are giving permission for these companies to follow you wherever you go. We then use this information to create mobility data trends in the country to produce our reports'[1]

1

While no further discussion has taken place about how this data is being shared, used or protected, Mexican civil society organisation (CSO), Red en Defensa de los Derechos Digitales R3D, has joined efforts with other Latin American

CSOs to demand that governments in the region protect the human rights of their population amidst the use of digital technologies during the COVID-19 pandemic. According to their pledge, the deployment of digital technologies must be commensurate with the benefits it might bring. In particular, the use of surveillance technologies to trace the virus transmission speed should be limited, time-sensitive, non-discriminatory and must adhere to basic privacy and data protection laws. In Mexico, a country where technology to track individuals has been used to spy on scientists, human rights defenders, political dissidents, journalists and other members of CSOs, including children, this should be a matter of concern.

Spyware in Mexico

In 2012, the Mexican government reported it had signed a $20 million deal with an Israeli-based company called NSO Group. NSO Group, which also goes by the name Q Cyber Technologies, is a company that develops and sells
2 technology to 'prevent and investigate terror and crime.'[2] The company's services are exclusively offered to government intelligence and law enforcement agencies under the explicit condition that they be used to fight terrorists and other criminal groups. As part of the tools offered by NSO, Pegasus is arguably amongst the most sophisticated spyware available on the market. According to an independent investigation conducted by research laboratory Citizen Lab (University of Toronto), Pegasus can infiltrate iOS and Android
186 devices by sending targeted text messages with malicious links. Once a mobile device has been infected, the spyware can access the target's private data, including passwords, contact lists, calendar events, text messages, and live voice calls from popular mobile messaging apps—including
3 WhatsApp.[3] The operator can turn on the phone's camera and microphone to capture activity in the phone's vicinity and use
4 the GPS function to track a target's location and movements.[4] This spyware was operational on the phone of one of the colleagues of Jamal Khashoggi, in the weeks prior to his extrajudicial execution.

An international investigation published in 2017—led by Citizen Lab, in collaboration with Article 19 and Mexican CSOs R3D, and Social Tic—identified dozens of cases in

which Pegasus was used to target human rights defenders, journalists, political opponents and members of civil society who were investigating high-level corruption or government involvement in human rights violations.[5] Some of the targeted individuals included investigative journalists as well as friends and relatives close to them. For instance, Carmen Aristegui and her son—a minor—were targeted, as well as colleagues and relatives of Javier Valdez, journalist and founder of newspaper Riodoce who was shot dead in May 2017 in Sinaloa. The investigation into the illegal use of spyware technology follows a 2016 study by Article 19, which confirms that during that year at least 53% of the reported 426 acts of violence and intimidation against Mexican journalists were linked to government officials.

Shortly after the publication of Citizen Lab's high-profile report, the Mexican government ordered an official investigation into the issue, but since then enquiries have stalled. Internationally, there is evidence that Pegasus may be in operation in more than 45 countries, and several litigations against NSO Group are still ongoing.[6] But this has not stopped the company from offering its services during the current pandemic.[7] Just recently, NSO Group has been 'pitching its tools as a means to help better understand how coronavirus is spreading.'[8] While the company emphasises that its employees will not have access to any data, it also says that its software will work best if a government asks local mobile network operators to provide the records of all subscribers in the country. Mexico, identified as one of the most dangerous places in the world to be a journalist, announced—as the lockdown began in April this year—that mobile phone companies were giving open access to data, so governmental institutions could monitor the attainment of social distancing measures in order to reduce the rate of transmission.[9]

In an era where track and trace mobile applications are being called upon to 'unlock' societies, we risk normalising the use of 'old' technologies to illegally pry into the most vulnerable in societies where by design there are no tools for accountability.[10] Technological responses are always political. The current legitimation of mass surveillance in polities where these tools have historically been used to

silence the voices of dissidents and human rights defenders is reckless. COVID-19 is a business opportunity for surveillance entrepreneurs. The situation asks us to critically engage with the deployment and development of technologies; but most importantly, the repurposing of surveillance technologies demands that we radically reimagine the governance of data and its links with justice in a post-pandemic world.

References

1. See: https://www.elfinanciero.com.mx/tech/google-y-apple-le-avisan-a-lopez-gatell-si-no-le-haces-caso-de-quedarte-en-casa
2. See: https://www.nsogroup.com/about-us
3. See: https://citizenlab.ca/2019/10/nso-q-cyber-technologies-100-new-abuse-cases
4. See: https://citizenlab.ca/2017/02/bittersweet-nso-mexico-spyware
5. See: https://www.nytimes.com/2017/06/19/world/americas/mexico-spyware-anticrime.html
6. See: https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries
7. See: https://citizenlab.ca/2018/12/litigation-and-other-formal-complaints-concerning-targeted-digital-surveillance-and-the-digital-surveillance-industry
8. See: https://www.bbc.co.uk/news/health-52134452
9. See: https://cdmx.gob.mx/portal/articulo/cierre-de-centros-comerciales-por-emergencia-sanitaria
10. Cruz-Santiago, A. (2020) Lists, Maps and Bones: The Untold Journeys of Citizen-led Forensics in Mexico. *Victims & Offenders.* 15:3, 350-369.

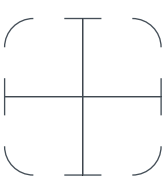
Arely Cruz-Santiago is a research fellow and co-investigator on the ESRC-funded 'Data Justice in Mexico's Multiveillant Society' project at the University of Exeter.


THE NETHERLANDS
TECHNO-OPTIMISM
AND
SOLUTIONISM

AS A CRISIS RESPONSE

Naomi Appelman, Jill Toh, Ronan Ó Fathaigh, and Joris van Hoboken

The COVID-19 pandemic and the government's containment response so far has resulted in a strengthening of existing techno-optimism and trust in experts in the Netherlands. Technology was already an integral part of government, in citizen-facing agencies and internally. Now, however, existing technologies are being repurposed and public–private partnerships are scrambling to develop *the* app with experts as final arbiters, and civil society, even though robust, fuelling the debates from the sidelines. In this crisis, experts seem to have primacy in charting the course, and technology is seen as the way to implement the measures. In the following, we will illustrate this in the areas of communication, health, policing, and contact tracing.



Communication

The use of communication technology has undergone a major transition in the Netherlands as a result of COVID-19 containment measures. This has included hundreds of thousands of employees working from home, and education moving online. There has been a debate over the communication platforms that are being used, with some universities banning the use of certain platforms such as Zoom over privacy concerns.[1] There has also been

1

controversy over online proctoring, where surveillance software allows the monitoring of a student's webcam, microphone, web traffic, screen, mouse and keyboard activity, and tracks movements to determine cheating.[2] Indeed, two student councils sued a university over the use of such software. However, in an important judgment, the District Court of Amsterdam ruled that the use of such software was not an unlawful interference with the right to privacy.[3] Notably, the Dutch Data Protection Authority has published advice on video-calling apps,[4] while admitting that it was not able to conduct 'extensive technical research' into the apps, and instead relied on information provided by the companies themselves. Further, in relation to social media platforms, the COVID-19 crisis has resulted in extensive reliance on dominant social media platforms by government agencies, health authorities, and police, including through paid online advertising. For example, a number of municipalities have been buying ads on Facebook to promote COVID-19 measures,[5] and various police forces have released videos on Twitter warning about disinformation.[6]

Health

Private–public partnerships can be observed in the digital healthcare sector, with increased efforts in data collection and sharing. First, Philips, two Dutch universities, and the Ministry of Health, Welfare and Sport (VWS) developed an online COVID-19 portal for hospitals to share patient data.[7] The crisis has propelled the state to allow the sharing of patient data without prior consent, a move that had previously been resisted due to privacy reasons. Second, a health app created by Amsterdam hospital OLVG and Luscii allows residents to enter their medical data and doctors to respond if they are suspected of coronavirus, to help hospitals cope with an influx of requests.[8] According to the OLVG, the app will eventually be available to 4.7 million people.[9] Lastly, medical universities and laboratories have been actively collaborating on the development of COVID-19 treatments, including the use of AI-based methodologies.[10]

There has been an increase of new actors and partnerships in the development and procurement of Personal Protective Equipment, in addition to the VWS and the National Institute

for Public Health and Environment (RIVM). In particular, the purchasing policy of the VWS regarding respiratory equipment has raised concerns amongst medical experts.[11] Issues regarding the procurement partners (i.e. the choice of Philips over existing partners), the potential compromising on quality of ventilators (i.e. prioritising speed and quantity over quality) and the lack of transparency in decision-making processes have surfaced. Private clinics[12] and independent organisations[13] have also supplied personnel, material and equipment to hospitals, but quality checks remain unknown.

Policing

Two factors are of importance in understanding the use of technology for the enforcement of COVID-19 measures. First, Dutch law enforcement already had a strong tradition of using technology to aid policing before the pandemic. The police have an extensive facial recognition system[14] with more than 2.2 million images, and use predictive heat maps[15] to allocate resources in large cities. Second, due to the extensive competencies of local governments, the enforcement of the containment measures is mainly organised locally.[16] These two factors mean that, even though the use of technologies for the enforcement effort is widespread, the picture of how technology is used in the enforcement of the containment measures is quite fragmented. The containment measures in the Netherlands were relatively relaxed in April and May 2020, allowing people to go outside in groups of up to three while maintaining a 1.5-metre distance, with violations incurring a €390 (440 USD) penalty.[17] The nature of these measures means the policing effort is focusing on the surveillance of public spaces, with drones,[18] scan-vehicles,[19] and cameras.[20] Municipalities are also using technology to facilitate citizen reports on violations of the social-distancing measures.[21]

Contact tracing

Finally, the Dutch government's efforts in developing a contact-tracing app through a rushed tender process and two-day 'appathon' (live-streamed on YouTube) have been widely deemed unsuccessful. An unfeasible timeline, and a lack of transparency, led to experts distancing themselves from the appathon.[22] Serious concerns about the procedure were raised by members of parliament, civil

23 society organisations, academics, and experts.[23] The Dutch Data Protection Authority as well as the government's legal counsel declared that the resulting apps did not meet data protection standards.

Wider concerns about the necessity of developing contact-
24 tracing apps have also been raised.[24] The concerns range beyond privacy, and include the potential social implications, respect for fundamental rights, adequate consideration
25 of European Council guidelines,[25] as well as the overall
26 effectiveness of any apps developed.[26] None of the seven coronavirus tracking apps tested in the appathon were deemed suitable for official use due to security flaws and data concerns. Nevertheless, the Dutch government has been insistent on developing an app, by since opting to
27 collaborate with technology giants like Apple and Google.[27] The involvement of Apple and Google has demonstrated the potential for exploitation of their dominant market positions when striking a balance between public objectives and their strategic interests as commercial companies. The use of mobile phones for contact tracing can also bypass democratic processes through their direct control of the dominant operating systems, which leaves no (or limited) room for citizen choice.

From this brief discussion, three concluding points can be made. First, that the techno-optimism and solutionism that was already present in Dutch society has surged in the present crisis, turning into a technological sideshow that has displaced wider discussions of the complex economic, social, and public health challenges of the pandemic. Second, the government's technology policies deployed during the crisis indicate pragmatism and effectiveness as apparent priorities, without much transparency about the underlying trade-offs. However, the importance of public values such as equality and privacy must also be taken into account, even under pandemic conditions. Only recently, The Hague District Court struck down the automated welfare-fraud detection system, SyRI, ruling that the government has a 'special responsibility' to guarantee fundamental rights during the application of new technologies. Finally, in spite of the 'death of experts' rhetoric as observed in many liberal

democracies, COVID-19 decision-making in the Netherlands has been largely delegated to a select group of scientific experts. This crisis has certainly highlighted the need for a discussion on the range of expertise that is considered in decision-making processes.

References

1. See: https://www.universiteitleiden.nl/en/dossiers/coronavirus-en/updates-en
2. See: https://nos.nl/artikel/2331075-kritiek-studenten-op-surveillancesoftware-voor-examens.html
3. See: https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBAMS:2020:2917
4. See: https://autoriteitpersoonsgegevens.nl/nl/nieuws/keuzehulp-privacy-bij-videobel-apps
5. For example Amsterdam, see: https://www.facebook.com/ads/library/?active_status=all&ad_type=all&country=NL&impression_search_field=has_impressions_lifetime&view_all_page_id=248022541905667
6. See: https://www.at5.nl/artikelen/200911/politie-waarschuwt-voor-nepnieuws-over-coronavirus
7. See: https://www.philips.com/a-w/about/news/archive/standard/news/articles/2020/20200415-philips-launches-national-portal-for-digital-exchange-of-covid-19-patient-data-in-the-netherlands.html
8. See: https://nos.nl/artikel/2331180-corona-check-app-van-olvg-nu-door-iedereen-te-gebruiken.html
9. See: https://www.parool.nl/amsterdam/olvg-app-meet-groei-corona-bijna-3000-officieuze-besmettingen-in-amsterdam~b9931b29
10. See: https://www.iamsterdam.com/en/business/news-and-insights/news/2020/amsterdam-institutions-ai-collaboration-coronavirus
11. See: https://www.ftm.nl/artikelen/aankooppolitiek-rond-beademing-verbijstert-deskundigen
12. See: https://www.parool.nl/amsterdam/amsterdamse-priveklinieken-stellen-personeel-en-faciliteiten-beschikbaar~b54773e8
13. See: https://www.coolblue.nl/hulptroepen
14. See: https://www.vice.com/nl/article/8xzydz/gezichtsherkenning-op-de-nederlandse-straten-moeten-we-dat-willen
15. See: https://zoek.officielebekendmakingen.nl/ah-tk-20142015-1321.html

16. See: https://www.ad.nl/binnenland/burgemeesters-krijgen-eerste-hand-in-handhaven-coronamaatregelen~ae1abbf2

17. See: https://www.rijksoverheid.nl/onderwerpen/coronavirus-covid-19/openbaar-en-dagelijks-leven/aanpak/groepsvorming-en-samenscholingsverbod

18. See: https://www.trouw.nl/binnenland/drones-controleren-of-u-zich-aan-de-coronaregels-houdt-maar-mag-dat-eigenlijk-wel~b3e551a4

19. See: https://beveiligingnieuws.nl/nieuws/rotterdam-zet-camerawagens-in-tegen-corona-overtreders

20. See: https://www.nu.nl/coronavirus/6041658/amsterdam-plaatst-extra-cameras-om-coronamaatregelen-te-handhaven.html

21. See: https://nos.nl/artikel/2328946-corona-overtredingen-melden-via-app-mensen-zelf-aanspreken-is-spannend.html

22. See: https://www.veiligtegencorona.nl/reactie-experts-selectieproces.html

23. See: https://www.veiligtegencorona.nl/#uitgangspunten

24. See: http://allai.nl/wp-content/uploads/2020/04/Online-versie-Brief-Minister-President-Rutte-Ministers-De-Jonge-Van-Rijn-Grapperhaus-de-heer-Sijbesma-inzake-COVID-19-tracking-en-tracing-en-gezondheidsapps.pdf

25. Recommendation C(2020) 2296 final of 8 April 2020: https://ec.europa.eu/info/sites/info/files/recommendation_on_apps_for_contact_tracing_4.pdf

26. See: https://nos.nl/nieuwsuur/artikel/2330937-kans-op-succes-corona-app-klein.html

27. See: https://www.rtlnieuws.nl/tech/artikel/5135056/ontwerp-corona-app-nederland-design-github

Naomi Appelman is a PhD researcher at the Institute for Information Law (IViR), University of Amsterdam.

Jill Toh is a PhD researcher at IViR.

Ronan Ó Fathaigh is a senior researcher at IViR.

Joris van Hoboken is a professor of law at the Vrije Universiteit Brussels and a senior researcher at IViR.


NORTH AMERICAN
INDIGENOUS PEOPLES
RUPTURED
KNOWLEDGE
ECOLOGIES

IN INDIAN COUNTRY

Marisa Elena Duarte

Fundamentally, the concept of data justice is ideal: it presupposes a reasonable state of information equity, where factual evidence and knowledge are thoughtfully integrated into decision-making. Sadly, for over two centuries before COVID-19, Indigenous peoples of North America have existed in a state of epistemic injustice. Even the points of negotiable agreement between sovereign tribes or *pueblos indígenas* and North American federal and state / provincial governments are clouded by misinformation and colonial disinformation about Indigenous rights and customs, land claims and boundaries, and rules around intellectual property and privacy. Nationalist systems subjugate Indigenous philosophies while excluding Indigenous families and communities from decision-making roles in public education, health care, and media. Specifically, in the US, leaders in sovereign Native nations have been excluded from decision-making roles around crafting the Coronoavirus Aid, Relief, and Economic Security (CARES) Act, which distributes billions of dollars to Americans and health care institutions. In Mexico, leaders of *pueblos autónomos* are not included in local health surveillance efforts. In Canada, leaders of sovereign First Nations have had to demand essential resources through parallel

governmental processes. While Indigenous leaders demand representation and participation, COVID-19 is exacerbating existing structural inequities in each of these contexts.

Lack of robust Internet and media infrastructure, accurate and precise epidemiological data and analyses, culturally relevant public health messaging, and means of data-sharing toward informed decision-making are contributing to the spread of COVID-19 through a number of Indigenous communities. Bigotry and ignorance amplify the stigmatisation of Indigenous peoples whose communities are suffering from outbreaks.[1] Where histories of redlining—including containment on reservations, reserves, and in remote pueblos—prevent Indigenous children from obtaining basic educational support, K-12 students rely on homework-by-mail to keep up with daily coursework.[2]

While technologically advanced societies hope for a vaccine, Indigenous government leadership struggles for inclusion in the negotiations between the federal governments and private industries that make PPE, clinical care equipment, vaccinations, and antiviral drugs deliverable and affordable through reputable institutions.[3] For some Indigenous leaders, this means working through intergovernmental bodies to pressure federal authorities to consider their treaty responsibilities to tribes. For others, it means working with non-governmental organisations, university labs, and mutual aid collectives to direct personnel, food, and PPE to tribal organisations. For others, it means writing letters to congressional or provincial representatives, and speaking with reliable journalists who can spread awareness of the crisis through media.

Considerations of data justice in Indigenous contexts require reflection on the range of information ecologies of Indigenous North America.[4] Presently, Indigenous knowledge—including information, datasets, and intellectual and cultural property created by and about Indigenous peoples—circulates through institutions such as tribal administrative offices, libraries and archives, museums, non-profit cultural centres, health centres, schools and universities, private corporations, and federal agencies via digital and analogue infrastructures and platforms. When information infrastructures work well

in terms of technical capacity, procedural routine, and skilled personnel, decision-makers can transmit, receive, craft, and push data, information, and knowledge through analogue and digital networks of humans and devices.

Regional epidemiological centres as well as tribal health centres typically have the means of receiving and sharing limited types of information relevant to clinical care and Indigenous community health. However, the first waves of COVID-19 outbreaks affected various regions so rapidly that prior means of communicating health information—including reliable health surveillance data and culturally targeted public health messaging—were quickly overwhelmed. In some regions, health providers have no training or systematic method for documenting cases of COVID-19 presenting in tribal clinics.

Through most of Mexico, health providers in *pueblos indígenas* have no tools for systematically counting and reporting cases of COVID-19 in areas with limited information and communication technologies. In the US and Canada, some tribal governments retain their own epidemiological data, whereas others report cases to states or provinces, and then rely on state health department or university epidemiological analyses. Divergent chains of reporting COVID-19 cases have resulted in different epidemiological calculations, where some account for spread through reservations and reserve communities, and some merely provide abstract analyses divorced from Indigenous geographies.

The relationship between (1) the functionality of institutional data-sharing assemblages and interfaces, (2) the capacity of individuals and institutions to create and disseminate health surveillance analyses and public health messaging at point of need, (3) practices of informed leadership, and (4) information integrity in a knowledge environment characterise any knowledge ecology structured around Indigenous health care. However, anecdotes emerging out of the waves of regional COVID-19 outbreaks throughout North America have revealed the weakened capacities of Indigenous communities' and governments' data-sharing infrastructures. Notably, these anecdotes reveal limitations

of technical capacity, data-sharing procedures, and skilled personnel who can assure the functionality of ICTs and data-sharing platforms as well as rapidly synthesise information for various stakeholders.

Furthermore, overall, systemic health inequities are compounded by federal abrogation of Indigenous treaty rights. In Canada, on March 23, 2020, the Assembly of First Nations executed a motion to declare a state of emergency with regard to the COVID-19 pandemic, including a call for federal, provincial, territorial, and municipal governments to systematically increase funding, support, and resources to First Nations, especially to remote and isolated communities. The state of emergency insists that 'First Nations leadership be fully and meaningfully involved at the decision-making tables in the development of all plans, legislation, policies, budget allocations and regulations regarding the COVID-19 pandemic federally and provincially, inclusive of the epidemiological datasets, budgetary spreadsheets, and other datasets that First Nations leaders can analyse with regard for the institutional capacities within their own governments.'[5]

The need to promulgate informed leadership as part of a state of emergency reveals existing structural inequities impeding the actionability of Indigenous data sovereignty, that is, the deliberate negotiated sharing of datasets across Indigenous and non-Indigenous institutions toward Indigenous well-being. In this context, Indigenous data sovereignty demands the dissemination of methodically assembled datasets affecting Indigenous well-being and livelihood across secure channels toward reputable and authoritative Indigenous institutions for analysis in accordance with Native scientific methodologies and tribal-centric policy-making.

However, in the midst of a fearful sociopolitical environment laden with governmental inequities, the means of carrying this out are challenged. Indigenous communities throughout Canada, the US, and Mexico are relying on non-profit organisations, grassroots activist collectives, and mutual aid organisations to raise emergency funds at a faster rate than governments can provide. Members of tribal communities and *pueblos indígenas* who are formally educated in

science, technology, policy, and health are voluntarily rapidly analysing, interpreting, and translating statistical analyses and mass media news updates about the virus, rates of transmission, fatalities, and economic impacts for their families, communities, and governments. The on-the-ground stories emerging out of First Nations communities reveal the depth of these challenges. In April the Yukon government, in support of a number of women's shelters and Indigenous health organisations, delivered 325 cell phones with 4-month service plans to women fleeing abusive relationships.[6] The effort is complicated by prior evidence showing that cyberstalking predicates abusive acts and assaults against First Nations women and girls.[7]

The effort is also complicated by digital divide research that shows the limitations of charitable efforts that drop un-sustainable Internet-ready devices and services into marginalised communities. For example, in this scenario, how will the recipients of these much-needed cell phones afford the comparable data plan after the subsidised 4-month period, particularly in light of the scientific likelihood that social distancing will need to occur for years until a vaccine is globally distributed, and employment options increase? While there is no doubt that these efforts are immediately appreciated, when it comes to data justice for First Nations and Metis peoples, subsidised cell phones and WiFi hotspots are like band-aids amidst the systemic and structural racism, including environmental racism, that marginalises Indigenous peoples through Canada's era of Truth and Reconciliation.

Meanwhile, in the US, President Trump's racist rhetoric and anti-scientific propaganda inflames the existing pub-lic health crisis in Indian Country. The lack of coherent messaging about COVID-19 from the White House has resulted in what US journalists are calling an infodemic: a parallel scourge of misinformation and disinformation about COVID-19 that is resulting in increasing viral spread as well as racist acts against social groups such as Asians and Asian-Americans (Trump refers to COVID-19 as the 'China virus'), and highly affected populations who already endure structural health inequities and systematic racism, including African Americans, Latinos, and Native Americans.

Since April 2020, Navajo Nation has been a hotspot for regional outbreaks that, due to the lack of social distancing and public health education, are moving through tribal and non-tribal communities across four states. Partisan politics fuels the outbreaks. While in New Mexico Democratic Governor Michelle Lujan extends periods of social distancing and storefront closures, and sends state resources to regional hospitals and clinics, attorneys are suing Arizona Republican leadership for massaging health data indicators in support of 're-opening the state', allowing for the operations of nursing homes state-wide as well as storefronts near Navajo Nation with little to no public health enforcement measures.[8]

8

Navajo Nation covers a massive territory, and multiple federal, state, and local health service providers, Internet service providers, chapter houses and district governments, and schools and colleges provide different levels of care to the region. Significant health information gaps occur through the lack of consistent epidemiological data-sharing and analyses across these institutions, including the state governments, Indian Health Services, regional private hospitals and clinics, and non-profit organisations. The lack of fibre optic cable to homes and anchor institutions both impedes deployment of emergency Internet hotspots in key locations, and makes it difficult or impossible for families to share information without traveling and speaking in person. Local authority figures, including fundamentalist church and spiritual leaders, white supremacist political movement leaders, and family leaders who are simply ignorant about what a virus is and how it is transmitted, disseminate misinformation and disinformation with fatal consequences.

Much of the news about what life with COVID-19 is like within and near Navajo Nation is distributed by independent Indigenous journalists in the region, who rely on their existing social networks to raise awareness of local challenges. Aspects of Navajo Nation's experience with COVID-19 reflect experiences in other sovereign Native nations throughout the US. Lummi Nation experienced outbreaks associated with intergenerational family gatherings. Though Oneida Nation and Menominee Nation issued shelter-in-place orders alongside the state of Wisconsin in early April,

within six weeks the state's Republican-led Supreme Court ruled that the governor's stay-at-home order was unlawful and unenforceable, effectively putting at risk millions of individuals, including tribal citizens.

In Mexico, on Sunday, March 8, the weekend before social distancing measures were announced by many US states, millions of women marched through cities and towns in protest of President Obrador's sexist response to systemic government mishandling of *femicidio*: significantly increasing cases of disappearances and assaults against women, including murders of feminists in particular.[9] Indigenous feminists and leadership supported aspects of this protest; a number of those disappeared and murdered are Indigenous activists.[10] Historically, Mexico's colonial ideology simultaneously subjugates women and Indigenous peoples through covert government-sponsored kidnappings and killings alongside corrupt church and government practices, including the withholding of hospital care and safe refuge, obfuscated or erroneous scientific datasets, withholding of technical reports, censorship of journalistic exposés, and general subjugation of information and knowledge pertaining to Indigenous peoples.

9

10

While Mexico is reporting the greatest number of COVID-19 cases in dense city centres such as Mexico City and Tijuana, scientists suggest that the government is not tracking or reporting the actual numbers of deaths, cases, and affected groups. Indeed, while the Mexican government closed the Mexico–US border in April to stem North–South contagion, the US and Mexican governments are now deporting hundreds of individuals likely exposed to COVID-19 in detention centres, most of whom are also Indigenous peoples from Chiapas and the Mayan communities in the borderland between Guatemala and Mexico.[11] Social stigmas compound lack of access to treatment and healthcare amongst the poorest sector of the national population. Officials are investigating the case of a Chiapas man who, in April, tested positive for the virus and shortly thereafter was found hanging from a tree outside his home in Ocosingo in an apparent suicide.[12]

11

12

In response to the economic recession across the NAFTA governments, local shop owners are price-gouging. Women's weaving collectives in Chiapas, grassroots Indigenous advocacy groups, and binational tribes such as the Pascua Yaqui Tribe / Yaqui people of Sonora have been raising funds and sending resources to families and the *pueblos autónomos* so that families can afford food staples amidst increasing joblessness.

Disinformation and misinformation also shape the public health response. In March, a Mexican political cartoonist released an image of a rural student wearing a face mask and standing outside his home holding a book, looking at a far-away city shadowed by a giant WiFi signal. The student says, loosely translated, 'Pardon me, Teacher, but I cannot hear you.' In April, the Yaqui people of Sonora made national news for their insistence on continuing annual Easter ceremonial traditions in spite of shelter-in-place warnings.[13] Advocates for Indigenous rights in Mexico have been supporting the cultural translation of public health messaging for the various Indigenous language communities throughout the country.

13

Throughout North America, only tribal governments with local technical and epidemiological expertise are maintaining and reporting datasets indicating numbers of cases and rates of transmission, and of those, very few are tracking cases in border towns and of individuals who are associated with the tribal community but who are not officially enrolled tribal citizens. One of the only ways for Indigenous leaders and health advocates to gather accurate and precise datasets is by reaching into their existing social networks to form secure data-sharing partnerships. Methods must include analyses of epidemiological data in light of Indigenous discernment of community social practices and norms, culturally informed contact tracing and public health education and messaging, local analyses of institutional barriers and opportunities, and tracing of viral spread through regions beyond government jurisdictions.

This approach requires a combination of relational skill, trustworthy productivity, political acumen, and scientific analytic expertise. It requires networks of teams who

can advocate for large structural changes, increase in infrastructure expenditures for Indigenous peoples and governments, and everyday social change through education and community awareness. By providing executive summaries of data-sharing activities and efforts with trusted policy-makers, in the future, authorities can advocate for the kinds of equitable data-sharing, research, and archival activities that need to occur through nation-to-nation negotiation between Canada, the US, Mexico, and *pueblos indígenas* and sovereign tribes. For now, though, throughout Indigenous North America, much of the work is about enduring and counteracting the brutality of the COVID-19 infodemic.

References

1. See: https://www.rollingstone.com/culture/culture-features/navajo-covid-racism-homelessness-1016763 and https://www.tandfonline.com/doi/full/10.1080/14631369.2020.1763161

2. See: http://nmindepth.com/2020/05/02/santa-fe-indian-school-pivots-from-digital-to-offline-learning-to-ensure-access-during-covid-19-pandemic and https://gemreportunesco.wordpress.com/2020/06/12/covid-19-pandemic-and-indigenous-and-non-indigenous-students-in-mexico

3. See: https://indiancountrytoday.com/news/tribal-leaders-share-relief-funding-challenges-0QKveBbwwE2cM2Nx5eY-KA and https://www.nationalobserver.com/2020/04/30/news/metis-treasurer-wants-seat-table-amid-covid-19-crisis

4. In sociotechnical systems theory, information flows across diverse institutions through networks of humans and devices, contributing to an ecology of routine and automated data-sharing as well as more specialized circulation of knowledges. As humans interact with, manipulate, and employ information toward their own agendas and needs, they imbue types of information—including data sets—with a quality of liveliness.

5. See: https://www.afn.ca/nc-bulletin-executive-motion-on-covid-19-state-of-emergency

6. See: https://www.cbc.ca/news/canada/north/yukon-women-free-phones-covid-19-1.5522386

7. Louie, D. W. (2017) Social Media and the Sexual Exploitation of Indigenous Girls. *Girlhood Studies.* 10 (2): 97-113.

8. See: https://www.azcentral.com/story/news/local/arizona-health/2020/04/07/arizonas-limited-coronavirus-data-sparks-frustration-confusion-lawsuit/2958629001 and https://www.abc15.com/news/local-news/investigations/attorneys-state-unlawfully-withholding-covid-19-information-using-false-facts

9. See: https://www.theguardian.com/world/2020/mar/09/thousands-mexican-women-protest-violence-murders-femicide-government-inaction

10. See: https://enlacezapatista.ezln.org.mx/2020/03/05/we-dont-need-permission-to-fight-for-life-zapatista-women-join-the-march-9-national-strike

11. See: https://www.npr.org/sections/coronavirus-live-updates/2020/04/15/834999661/official-alleges-the-u-s-has-deported-many-covid-19-positive-migrants-to-guatema and https://www.newsweek.com/mexico-health-officials-say-new-coronavirus-cases-coming-people-crossing-us-border-1506199

12. See: https://www.eluniversal.com.mx/estados/tras-dar-positivo-covid-19-hombre-presuntamente-se-suicida-en-chiapas

13. See: https://www.jornada.com.mx/ultimas/estados/2020/04/11/realizan-yaquis-del-coloso-sus-rituales-de-cuaresma-5720.html

Marisa Duarte is an assistant professor with the program in Justice and Social Inquiry through the School of Social Transformation at Arizona State University.

NORWAY

SMITTESTOPP

SMITTESTOPP:

THE RISE AND FALL

OF A TECHNOFIX

Kristin Bergtora Sandvik

This short case study looks at the making of the 'Smittestopp' ('stop transmission') app in the period March–June 2020 as a public health tool intended for the Norwegian COVID-19 response.[1] Norway is a COVID-19 success story. It closed schools, businesses and international travel in mid-March, and significantly restricted freedom of movement within the country. Despite being 'unprepared' for a (predicted) pandemic, the health sector has coped. By the first week of April—amidst concerns about the skewed impact on immigrant populations[2]—the outbreak was declared to be under control.[3] The subsequent impact has been comparatively mild. At the end of April, of a population of 5.4 million, there were 7,669 confirmed cases, 209 deaths and a total of 169,124 individuals tested. By mid-June, there were 8,606 confirmed cases, 242 deaths and a total of 277,253 individuals tested.[4] While this forceful response had immediate and severe implications for the Norwegian economy, the impact is widely expected to be partly mitigated through use of the country's sovereign wealth fund.[5]

The following is an initial attempt to critically conceptualise the rise and fall of the Smittestopp app as a specific cultural project and a domestic human rights issue, drawing on

Norwegian language media reports, social media entries, expert communication, government reports, and public health communication. It also builds on my ongoing work on tracking devices, digital bodies and experimentation in humanitarian aid.[6] I am a native Norwegian speaker and all translations are my own. Methodologically, this mapping exercise has been an almost impossible project, with events overtaking scholarly analysis at every turn. However, I believe that capturing the development and critical reception of the Smittestopp app in real time, and as it unfolded, can be a valuable starting point for academic analysis and policy evaluation of this particular app, as well as of the COVID-19 tracing app ecosystem and its discontents.

From late April, the lockdown was gradually eased, coinciding with the launch of the Smittestopp app. Culturally and politically, much of the response and the success of social distancing rules have been organised around a widespread trust in government and public health authorities, particularly the Norwegian Institute of Public Health (FHI). Central here is the deeply ingrained cultural concept of *dugnad* derived from the old Norse *dugnað* meaning unpaid and voluntary work carried out collectively.[7] Norway has a highly advanced digital economy, and Norwegians are quick and trusting technology adopters.[8]

On April 16, after about a month of research and development, the Norwegian government launched the Smittestopp app,[9] developed by the governmental research company Simula on behalf of the FHI.[10] The objective of the app was to 'see who has been in the proximity of infected persons, thus helping to curb transmission.'[11] In the official communication, Smittestopp was presented as 'an app that helps the health authorities curb transmission through anonymised information about movement, which is then used to develop effective infection control measures.'[12] Prime minister Erna Solberg stated that 'Personally, I believe that if we are to get our everyday life and freedom back, as many people as possible need to download the app.'[13] The FHI poster for the app proclaimed that 'Together, we can

combat COVID-19. Get notified if you have been in contact with infectees. Download the app.'[14] Downloading the app is thus considered a fulfilment of the civic duty to contribute to the *dugnad* (community work): 'If enough people use the Smittestopp app, it will help to reduce the number of people who become ill as a result of the coronavirus.'[15] By April 27, 1.5 million Norwegians had downloaded the app.[16] However, only 899,142 actually activated it.[17] In early June—in the context of an emergent consensus that the initial version of Smittestopp had not been successful, with only a little over half a million active users—Smittestopp and FHI began testing a new version of the app based on the Apple–Google solution.[18] A very short time later, the government pulled the plug on Smittestopp, and announced that it would split the app in two, and adopt the Apple–Google solution.

For comparative purposes, the rest of this case study considers three aspects of the initial version of Smittestopp: attributes, timeline, and an inventory of critical issues identified by the domestic technology and data protection communities.

The attributes of Smittestopp

In an English language explainer, the app's function was described as follows:

> 'When you are in close contact with another person who has the Smittestopp app on their smartphone, the apps will send signals to each other. If the other person has coronavirus disease, the app will remember that your phone has been in close contact with them. You will then receive a text message explaining what you should do to ensure that you do not pass on the infection and advice to help you look after your health. You will not be told who was ill with coronavirus disease, only the date on which you were in close contact with them.'[19]

A technical explanation of downloading procedures and privacy policies then followed. The explainer stated that 'You must be aged 16 or over to use the Smittestopp app.

Your data will be stored in a data cloud for 30 days.' Much less communicated was the second functionality of Smittestopp, namely that the data were also collected for research, to which this time limit did not apply. Finally, the explainer emphasised that 'you can erase your data in
20 Smittestopp at any time. You can delete the app at any time.'[20]

Although the source code was not available, it is known that it was different from the Apple–Google approach, which collects data locally. Smittestopp collected both GPS and Bluetooth data and used centralized, non-anonymous
21 storage and management to produce anonymised statistics.[21] The data were stored in Ireland, on the Microsoft-owned cloud computing platform Azure, and controlled by the
22 Norwegian government.[22]

When the app was launched, the threshold for activating the proximity function was over 15 minutes of contact within a
23 range of two metres.[23] It was announced that the SMS alerting function would only work after a period of experimentation and testing, including calibration of the number of minutes' proximity that would be required to record a contact event. FHI has acknowledged in hindsight that it was 'borderline
24 irresponsible to launch the app so rapidly'.[24] However, at the time of the launch, through an unusually insistent form of public communication, Simula, FHI and the Minister of Health all insisted that there were no problems with the app, and that downloading it would be instrumental to 'saving lives'.

Timeline

Smittestopp is deeply embedded in the rapidly unravelling ecosystem of Covid-19 tracing apps: it is a direct offshoot of the Science paper by Ferretti et al. (2020) and the work by Prof. Christopher Fraser at the University of Oxford. In early March, Fraser promoted the idea of an app to the powerful Director of the Research Council of Norway, a former FHI employee, who subsequently convinced the
214 FHI director that this was a good idea, resulting in a very rapid and exceptionally opaque research and development process. Quite *how* Simula was able to land a contract with the government—despite seemingly little experience of designing apps, epidemiology, or handling sensitive data—

should be the subject of further interrogation. By March 11, Simula was already offering its services for free to FHI, and by March 16, Simula had obtained a legal opinion as to how it could avoid a public tender process[25].

The budget for the app was 45 million Norwegian kroner (4.7m USD); Simula's contract was for 16 million (1.6m USD), including subcontractor agreements. Weeks after the R&D began, the app got a legal basis in the regulations of digital infection tracing of March 27 (valid until December 1, 2020).[26] The regulations gave a detailed list of the type of personal data to be registered in the Smittestopp tracking system. This included mobile phone numbers, age, location data, and proximity to / contact with infected individuals. Personal data from this system could be linked with a range of governmental databases. Importantly, the regulations contained a number of restrictions on purpose limitation and mission and function creep, including commercial use and sharing with law enforcement or the judicial system. The regulations also contained rules on deletion, which attempted to distinguish between the deletion of personal data after 30 days and longer retention of data for research purposes. Initially, the plan was that the testing phase would be completed in May 2020, and the SMS alerting function activated thereafter. As it turns out, Smittestopp never alerted anyone and did not save any lives. Part of the explanation is that Norway got the outbreak under control at a relatively early stage. Nevertheless, throughout its short lifespan of 8 weeks, Smittestopp was subjected to a barrage of criticism. Taking stock of these criticisms is important if we are to learn from the Smittestopp case, and also for comparative analysis of technology-driven responses to COVID-19. I have outlined the main criticisms in the following.

25

26

Hasty development and unclear purpose

The first criticism concerned the lack of clarity about what the app did and was supposed to do, as its functionality, implementation, and use by the public continued to evolve. The app had, literally, been developed in 'record time' (only 4.5 weeks) when it was launched in mid-April 2020. In the first release of the app, there were problems of functionality and high battery use. Users perceived the downloading

process to be complicated and downloading attempts frequently resulted in failure. The GPS/Bluetooth solution was controversial from the start.

The app was intended to support not only infection tracing, but also research about population movement underpinned by an explicit wish to measure changes in behaviour following new government rules. There were explicit concerns about data leakages and mission and function creep: that the app collected much more information than it needed to perform infection tracing. Many weeks into the app's deployment, the solutions for anonymising data for research purposes were not fully developed. Even if you removed information about phone numbers and the individual user IDs, specific location data—in a sparsely populated country—would have been sufficient to identify individuals. The Smittestopp solution was seen by critics as unnecessarily intrusive, as the data was
27 moved from phones to the central server on an hourly basis.[27]

While Simula and FHI (as well as the regulatory framework) all emphasised that data would not be shared, or that data would be used by government bodies for other purposes than those originally envisioned—and that 'Simula will not
28 commercially benefit'[28]—both institutions are situated within larger international networks. An attempt to use the Freedom of Information Act to gain insight into the source code was rejected with reference to possible commercial value based on international interest in the code, which could potentially
29 have been made available through a license system.[29] Later, Simula pitched Smittestopp in at least one international
30 tender process.[30]

Because the project had not been put out for tender by the FHI, a formal complaint to KOFA, the appeals board for public procurement, was submitted by members of the
31 domestic tech community.[31] The issue of contestation was whether the requirement for exemption from the tender
 regulations, that the app is 'essential' was fulfilled. The FHI based its argumentation on paragraphs 13-3 (force majeure) and 13-4 (the need for rapid delivery due to concern for the population's life and health) in regulations on public
32 procurement.[32] While Simula is on record making the initial

contact with FHI (as evidenced by a freedom of information act request documenting the Simula pitch of March 11 as well as interviews given by Simula) a development contract between FHI and Simula—affirming that FHI had approached Simula with a view to producing a tracing app and not the other way around—was only signed on April 8. The contract for operation and maintenance was signed on April 16.[33]

Security

The use of SMS as a channel of notification was criticized as a potentially significant vulnerability. According to the developers, this solution was chosen because an SMS was a 'simple solution' which everyone 'knows how to respond to'. The idea was that the app was going to be simple and quick to develop.[34] According to critics, spoofing—the falsification of sender address and text messages—was a low-hanging fruit for malicious agents. And fake SMS content could scare people if they received messages imploring them to report to a hospital (further traumatising vulnerable people), or if they were prompted to visit fake websites that requested sensitive personal and financial data. A more technical criticism was also levied against the closed source code approach, which, it was argued, would hinder white-hat hackers in offering assistance by hacking it *first.*[35] In tandem with this, there were concerns about poor risk assessments and Simula's suggestion that security testing could happen in 'a controlled manner' once the app was launched.

Concerns about distributive impact

There were also concerns about indirect impact, particularly on labour relations, access to justice, and freedom of the press. While there was considerable official pressure to download the app, according to labour law experts, a Norwegian employer could not require that employees download it. Employers could even (for information security reasons) prohibit downloading the app onto a mobile phone belonging to the employer.[36] Nevertheless, the pressure to download the Smittestopp app was likely widespread amongst employers. Moreover, Norwegian newspaper editors and lawyers expressed concern about source protection and client confidentiality[37]—all issues in urgent need of further inquiry.

Will it work and for what?

Finally, from the start, there were concerns about *whether* the app would work. Security expert Bruce Schneier appeared on the front page of the main Norwegian business newspaper
38 to declare that 'the app is meaningless'[38] pointing to the question of what one would actually do with an SMS alert, given contact—defined as a proximity of two metres for a certain length of time—is not the same as transmission. A related issue was the wiggle room in producing a social reality of 'usefulness'. With disease reproduction rates below
39 one,[39] the issue of 'production targets' once the testing phase had been completed and the full functionality of the app was put in place remained unclear throughout. The developers argued that the testing phase of the Norwegian
40 approach[40] (i.e. a rapidly developed work-in-progress tracing tool) –concomitant with a full roll-out across the country— was a strength, given it allowed for increasing or decreasing thresholds of time (e.g. from 5 to 20 minutes) and physical distance (e.g. from one to five metres). A key feature here is the inherent flexibility of these thresholds: adjusting the thresholds could radically alter the number of people being notified, thus contributing to an increase in the app's relevance as an infection tracker. Nonetheless, a month after the April 16 launch, it was reported that the
41 app had helped discover no infected individuals,[41] despite
42 collecting nine billion GPS positions.[42] In early June, as the number of Smittestopp users continued to plummet, the Minister of Health emphasized that even if only a few people used the app, the data collected were very important to analyse the spread of the pandemic, the effects of public
43 health interventions, and to optimize infection tracking.[43] The intrinsic connection between downloading, *dugnad*—or community working—and saving lives was no longer present in the government's communication.

The public discourse, a human rights failure and the end of Smittestopp

The launch of Smittestopp was followed by vigorous and highly public debate, with domestic security, legal, and IT security experts all weighing in. Persistent problems with the technical and legal aspects of the app, Simula's increasingly defensive and aggressive attitude (including

assertions that critics were 'unpatriotic', or—in the case of this author—'dishonest'), and the passivity of the institutions who normally claim the mantle of being watchdogs, eventually mobilised the Norwegian tech community to publish a joint statement on contact tracing, taking an unprecedented step in the direction of collective action.[44] If this were to signal the emergence of a new civil society actor, it would be a highly welcome legacy of Smittestopp.

44

However, for the purposes of democratic deliberation, we also need to learn more about the things that do not seem to have worked well. Conspicuously absent from the debate throughout March, April, May and June was the entire Norwegian human rights community—academics, government institutions and civil society actors included—who loyally lined up behind the *dugnad* and did nothing to hold FHI and Simula publicly to account for launching a massive humanitarian experimentation project on the Norwegian population.[45] The Director of the Norwegian Helsinki Committee went the furthest, going so far as to proclaim 'A Human Rights yes to the Smittestopp app' the day after its launch, on April 16.[46] On April 28, the head of Amnesty International Norway wrote an op-ed in the main daily tabloid arguing that Smittestopp was 'a mild breeze compared to the kind of surveillance that is being rolled out across the world'.[47]

45

46

47

Nevertheless, on June 16, the Amnesty International Security Lab based in Berlin launched a report describing the apps from Bahrain, Kuwait and Norway as the world's worst on privacy, having 'run roughshod over people's privacy, with highly invasive surveillance tools which go far beyond what is justified in efforts to tackle COVID-19.'[48] While the Norwegian data protection authorities undertook several investigations into the technical make-up of the app itself,[49] and in the end were instrumental in killing the app on June 15,[50] there is a widespread perception that they acted too timidly for too long, and when they finally acted, it was perceived as an overdue reaction to an already failed product. According to Amnesty International, it was only after seeing *their* report on June 2 that the Norwegian government and data protection agency moved into action.[51]

48

49

50

51

In a time of global tech capitalism and undemocratic data governance, caring about human rights at home and daring to ask uncomfortable questions is key to the credibility of the human rights community. The lesson from Smittestopp is that this kind of alertness and courage is also required in Norway. That is what *dugnad* should be all about.

References

1. The invitation to write this entry has resulted in two blog posts in Norwegian and English and a longer case study entitled 'Smittestopp': if you want your freedom back, download now' (*Big Data & Society* 2020). I am grateful to the editors for the opportunity and encouragement.

2. See: https://blogs.prio.org/2020/04/migrants-and-covid-19-in-norway-five-reflections-on-skewed-impacts

3. See: https://www.reuters.com/article/us-health-coronavirus-norway/coronavirus-epidemic-under-control-in-norway-health-minister-idUSKBN21O27H

4. See: https://www.fhi.no/en/id/infectious-diseases/coronavirus/daily-reports/daily-reports-COVID19

5. See: https://www.regjeringen.no/en/aktuelt/the-government-acts-to-mitigate-effects-of-the-covid-19-pandemic-on-the-economy/id2693471

6. Sandvik, K.B. (2019) Making wearables in aid: Digital bodies, data and gifts. Journal of Humanitarian Affairs 1(3): 33-41 DOI: https://doi.org/10.7227/JHA.023 ; Sandvik, K.B. (2020b) Wearables for something good: aid, dataveillance and the production of children's digital bodies. Information, *Communication & Society* 1-16. DOI: https://doi.org/10.1080/1369118X.2020.1753797 ; Sandvik, K.B. (2020b) Digital Dead Body Management (DDBM): Time to Think it Through. *Journal of Human Rights Practice.* huaa002, DOI: https://doi.org/10.1093/jhuman/huaa002

7. See: https://snl.no/dugnad

8. See: https://www.norway.no/en/missions/eu/about-the-mission/news-events-statements/news2/desi-report-norway-2-on-digitalization-in-europe

9. See: https://www.thelocal.no/20200416/norway-launches-smittestop-app-to-track-coronavirus-cases

10. See: https://www.simula.no/news/smittestopp-klar-nedlastning

11. See: https://www.nrk.no/nyheter/lanserer-app-for-smittesporing-1.14984326

12. See: https://helsenorge.no/smittestopp#Sp%C3%B8rsm%C3%A5l-og-svar-om-appen

13. See: https://www.vg.no/nyheter/innenriks/i/P9xGAJ/solberg-hvis-vi-skal-faa-hverdagen-tilbake-maa-flest-mulig-laste-ned-appen

14. See: https://www.fhi.no/contentassets/4e82300b73164e358e0dfbef96db8fa4/smittestopp-plakat-a3.pdf

15. See: https://helsenorge.no/SiteCollectionDocuments/korona/smittestopp-explainer-engelsk-2020-04-24.pdf

16. See: https://www.nrk.no/nyheter/nesten-1_5-millioner-nedlastinger-1.14997489

17. See: https://www.fhi.no/sv/smittsomme-sykdommer/corona/nokkeltall-fra-smittestopp and https://www.digi.no/artikler/veksten-i-bruken-av-smittestopp-appen-har-nesten-stoppet-opp/491145

18. See: https://www.digi.no/artikler/ny-versjon-av-smittestopp-appen-skal-testes/493569

19. See: https://helsenorge.no/SiteCollectionDocuments/korona/smittestopp-explainer-engelsk-2020-04-24.pdf

20. See: https://helsenorge.no/SiteCollectionDocuments/korona/smittestopp-explainer-engelsk-2020-04-24.pdf

21. See: https://www.fhi.no/sv/smittsomme-sykdommer/corona/slik-har-fhi-utviklet-smittestopp/#google-og-appleinitiativet

22. See: https://www.aftenposten.no/kultur/i/GGL7vq/forklart-smittestopp-myndighetenes-smitteapp

23. See: https://helsenorge.no/smittestopp#Sp%C3%B8rsm%C3%A5l-og-svar-om-appen

24. See: https://www.nrk.no/norge/fhi-direktoren_-_pa-grensen-til-uforsvarlig_-a-lansere-smittestopp-appen-sa-fort-1.15054567

25. Sandvik (2020) 'Smittestopp': if you want your freedom back, download now. *Big Data & Society.*

26. Forskrift om digital smittesporing og epidemikontroll i anledning utbrudd av Covid-19. See: https://lovdata.no/dokument/LTI/forskrift/2020-03-27-475

27. See: https://www.medier24.no/artikler/den-nye-smittestopp-appen-er-et-redskap-i-det-godes-tjeneste-sa-hvorfor-er-vi-skeptiske/490997

28. See: https://khrono.no/simula-vil-ikke-tjene-penger-pa-smittestopp-app/479935

29. See: https://khrono.no/simula-vil-ikke-tjene-penger-pa-smittestopp-app/479935

30. See Sandvik (2020) 'Smittestopp': if you want your freedom back, download now. *Big Data & Society.*

31. See: https://www.klagenemndssekretariatet.no/klagenemda-for-offentlige-anskaffelser-kofa

32. See: https://www.anbud365.no/bransjer/helse-omsorg/smittestopp-appen-klaget-inn-for-kofa-kofa-medlem-med-stotte-til-innklagede/ FOA § 13-3 e jfr § 13-4 a; https://www.digi.no/artikler/kommentar-hastekjopet-av-smittestopp-appen-er-antakelig-ulovlig-uansett-er-det-darlig/490451 ; https://lovdata.no/dokument/SF/forskrift/2016-08-12-974

33. See Sandvik (2020) 'Smittestopp': if you want your freedom back, download now. *Big Data & Society.*

34. See: https://nrkbeta.no/2020/04/20/sa-enkelt-er-det-a-forfalske-sms-er-fra-smittestopp

35. See: https://www.digi.no/artikler/kommentar-simula-ma-redegjore-for-sikkerheten-til-smittesporings-appen/489462

36. See: https://www2.deloitte.com/no/no/pages/legal/articles/kan-arbeidsgiver-palegge-bruk-av-smittestopp-appen.html

37. See: https://www.vg.no/nyheter/meninger/i/dO14rO/app-app-app

38. See: https://www.dn.no/teknologi/koronaviruset/regjeringen/smittevern/verdenskjent-sikkerhetsekspert-slakter-meningslos-norsk-smitteapp/2-1-793535

39. See: https://www.aftenposten.no/norge/i/vQ2wxB/fhi-med-nytt-anslag-over-smittespredningen-i-norge-naa-stiger-usikkerheten-kraftig-igjen

40. See: https://helsenorge.no/smittestopp#Sp%C3%B8rsm%C3%A5l-og-svar-om-appen

41. See: https://www.dagbladet.no/nyheter/har-ikke-oppdaget-coronasmitte/72454590

42. See: https://nrkbeta.no/2020/05/13/smittestopp-samler-inn-samme-type-data-som-i-nrk-avsloring

43. See: https://www.digi.no/artikler/under-15-prosent-bruker-smittestopp-appen/493513

44. See: https://medium.com/@jointstatementnorway/joint-statement-on-contact-tracing-for-norway-331ee49fc6f6

45. Sandvik (2020) 'Smittestopp': if you want your freedom back, download now. *Big Data & Society.*

46. See: https://www.vg.no/nyheter/meninger/i/zGJjKK/et-menneskerettslig-ja-til-smittesporing

47. See: https://www.facebook.com/AmnestyNorge/posts/10157309146578652

48. See: https://www.amnesty.org/en/latest/news/2020/06/bahrain-kuwait-norway-contact-tracing-apps-danger-for-privacy

49. See: https://www.datatilsynet.no/aktuelt/aktuelle-nyheter-2020/starter-kontroll-av-smittestopp

50. See: https://www.theguardian.com/world/2020/jun/15/norway-suspends-virus-tracing-app-due-to-privacy-concerns

51. See: https://www.amnesty.org.uk/press-releases/bahrain-kuwait-and-norways-contact-tracing-apps-among-most-privacy-infringing

Kristin Bergtora Sandvik is a professor of legal sociology at the Faculty of Law, University of Oslo, and research professor in Humanitarian Studies at PRIO.


THE PHILIPPINES
FAST TECH
TO SILENCE
DISSENT,

SLOW TECH FOR PUBLIC HEALTH CRISIS

Vino Lucero

Already behind most jurisdictions in the region, the Philippine government has been having a hard time bringing its information systems into the 21st century. Technology upgrades were never a priority for most government agencies, as most would rather spend on improving daily frontline services than invest in something that they do not see as immediately beneficial for their stakeholders. The prejudice against spending for technology might have been the same when the administration brainstormed about how to spend its PHP 353.86 billion (7.06bn USD) COVID-19 budget. Most went to cash-aid and medical services,[1] while technology for good[2] faded into oblivion. 1, 2

With hundreds of millions already going to surveillance funds[3] from the annual budget, technology might be the government's weapon of choice for maintaining control of public sentiment through silencing dissent, but not for 3

addressing the COVID-19 pandemic. Explicit bias towards the well-connected was also apparent in the process of choosing external technology partners, despite overwhelming volunteer interest across the technology and civil society sectors. This bias, however, was not followed by due diligence in ensuring that the partnerships would yield the desired results.

Lockdown now, tech later

The use of technology to assist in the COVID-19 response has therefore appeared to be more of an afterthought for the Philippine government. While the first local case was recorded
4 on March 7[4] and lockdowns in highly urbanised cities started
5 in mid-March,[5] high-level conversations on COVID-19 tech solutions only started in the first two weeks of April.

As mentioned, the Philippine government chose to collaborate with established technology companies who had already worked on government projects or that had extensive private sector connections. Some deals were done
6 without proper technical vetting or effectivity checks[6] from supposed government monitors. The lack of proper vetting, in turn, caused local IT experts to raise concerns over excessive permissions user data permissions and post-pandemic data custody in relation to the official contact-tracing
7 app.[7] Indeed, the data collected data may be used for other purposes like the 2022 Philippine elections, given the vagueness of the app's privacy provisions.

Another worrying aspect is a lack of systems integration, resulting in individual data silos for each platform. The work of integrating existing technological systems and platforms for COVID-19 response and monitoring also came as an afterthought, with differences in systems development being a key hindrance to making the integration smoother.

Those excluded from official technology initiatives, meanwhile, stepped up to craft independent monitoring and analysis tools to increase citizen awareness of national and

subnational COVID-19 situations. Civil society organisations, even those with limited technological ability, used common technology-powered tools and applications to design budget and procurement monitoring systems,[8] relief operations systems, and other COVID-19 response initiatives that the government is otherwise failing to address.

Data in disarray

Data issues—as well as questionable data interpretation from the country's top leaders—have also cast a shadow over how tech can positively impact COVID-19 policy-making and response. It appears that data are being played to fit preferred narratives of flattening the curve to elicit favourable citizen feedback, while in reality, the drop in publicly reported coronavirus cases has actually been caused by problems with data validation and misreporting. Errors and discrepancies in anonymised COVID-19 data[9] were earlier uncovered by experts from the country's top university, prompting one senator to observe that 'garbage data' could lead to 'garbage decisions' from the Philippine government.[10]

Press statements by presidential appointees related to COVID-19 have also led to confusing and inaccurate interpretations of official data, with some even releasing statements directly contradicting the analysis of data and technology experts. The country's health secretary has also claimed that the Philippines has flattened the curve on new local transmissions and now entered the second wave of the health crisis[11]—contradicting the reported data of his own office.

The presidential spokesperson, meanwhile, has spun testing capacity data to exaggerate government achievements by using estimated maximum capacity instead of actual testing capacity.[12] This made it appear that the Philippine government was able to test more than three times its actual capacity.

But these blunders pale in comparison to the biggest lapse of all: delayed COVID-19 data validation.[13] This issue, allegedly due to the shortage of hired encoders in the early months of the health crisis, resulted in a mix of new and old reports of COVID-19 cases that rendered daily COVID-19 bulletins

as merely a toll count rather than an accurate depiction of trends for new cases. A case in point: on the day the Philippine president announced that most of the highly urbanised cities would be opened up after more than two months of strict lockdown with no mass testing, it also reported the highest single-day number of verified COVID-19 cases since the pandemic started[14], a significant number of which are old cases who have just been recently confirmed by newly hired validators.

Louder on silencing dissent

While much work remains to be done to improve its COVID-19 response, the Philippine government has been relentless in using technology to silence dissenting voices—at the same time pushing its political agenda to a distracted constituency. Following through with existing COVID-19 initiatives has taken a back seat, as technology is being used more as a tool for curtailing freedom of expression rather than for addressing issues related to the pandemic.

This reality is consistent with the government's legislative priorities, with the congress hastily passing an anti-terror bill with provisions that gives it excessive discretion and eases the burden of proof for police on surveillance and imprisonment of suspected terrorists;[15] which may be twisted to include government critics. The National Bureau of Investigation has also been using technology to monitor criticisms from ordinary citizens against the president[16] in the guise of implementing the full force of the law, while giving compassion and due process to administration allies violating provisions on spreading disinformation during the COVID-19 pandemic.[17] The Philippine government also had the time to launch an online signature campaign to support its bid for constitutional reform and shift towards federalism using the gov.ph domain.[18]

Meanwhile, the country's top legal defender barred continued operations of the broadcasting network ABS-CBN,[19] which has been attacked and criticised by the president since 2016. *Rappler* executive editor Maria Ressa was also convicted by a Manila court of cyber libel charges—with the help of the Justice Department in using an archaic law to ensure the viability of the complaint.[20]

With all these recent developments considered, it is apparent that technology is not being used well to tackle the spread of COVID-19 in the Philippines. Instead, it is being used to fight freedom of expression, press freedom, and justice. All while government coffers are being emptied to supposedly respond to the pandemic—with the executive having nothing concrete to show for it thus far.

References

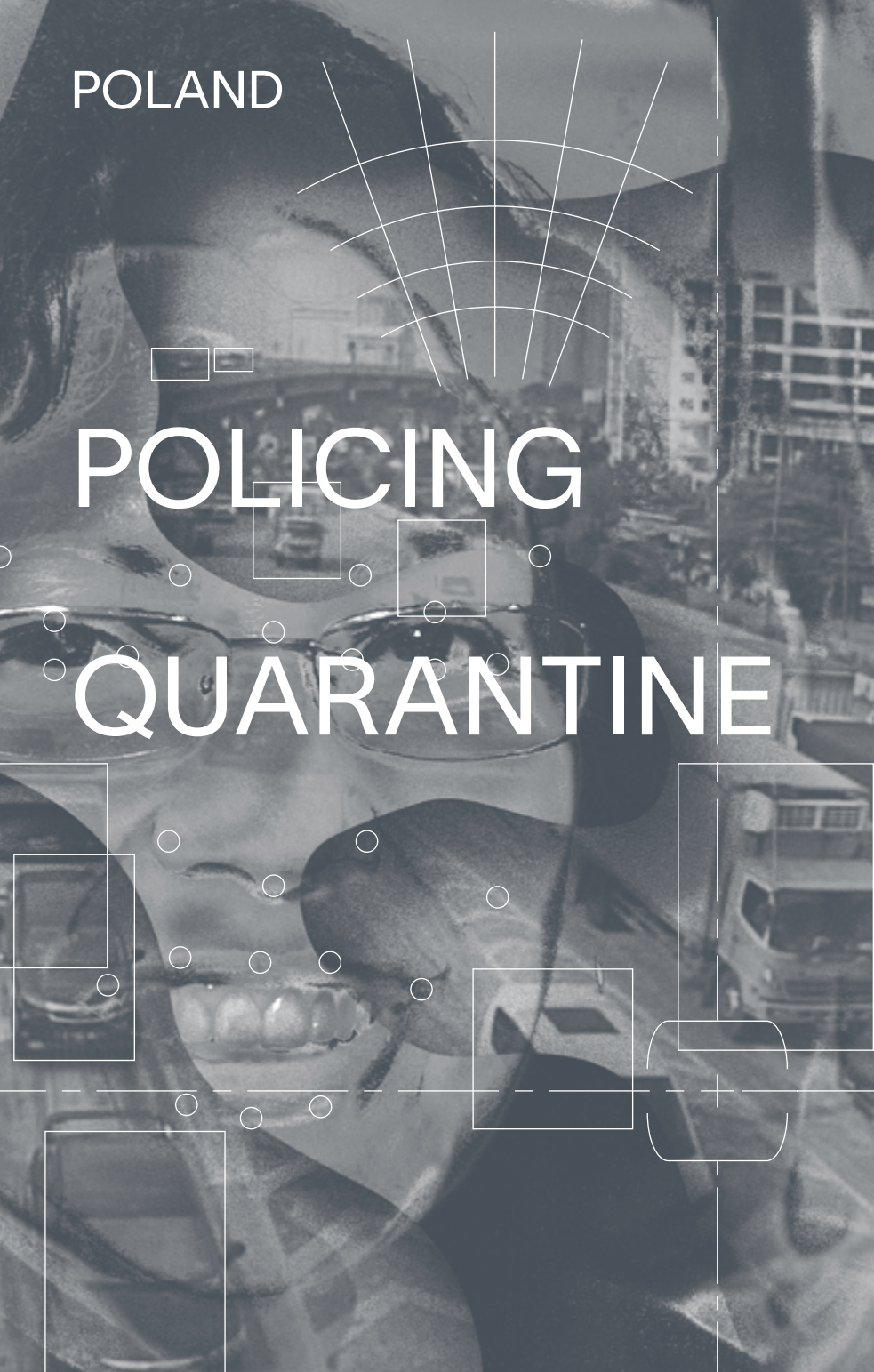
1. See: https://cnnphilippines.com/news/2020/5/28/covid-19-budget-breakdown.html
2. See: https://techforgoodhub.co.uk/tech-for-good
3. See: https://www.rappler.com/newsbreak/in-depth/251038-confidential-intelligence-funds-government-agencies-dict-2020
4. See: https://www.philstar.com/headlines/2020/03/07/1998804/philippines-has-first-local-case-covid-19
5. See: https://www.rappler.com/nation/254101-metro-manila-placed-on-lockdown-coronavirus-outbreak
6. See: https://opinion.inquirer.net/130935/rios-revelations
7. See: https://www.rappler.com/newsbreak/in-depth/263090-borderline-spyware-information-technology-experts-alarm-stay-safe-app
8. See: https://news.abs-cbn.com/ancx/culture/spotlight/05/01/20/this-kid-created-a-budget-tracker-that-traces-where-government-funds-for-covid-19-goes
9. See: https://newsinfo.inquirer.net/1273838/lapses-in-doh-patient-data-uncovered
10. See: https://newsinfo.inquirer.net/1274217/some-senators-hit-doh-after-experts-flag-alarming-errors-in-covid-19-patient-data
11. See: https://www.philstar.com/headlines/2020/05/21/2015565/duque-walks-back-second-wave-remark-after-garnering-criticism
12. See: https://cnnphilippines.com/news/2020/5/25/Philippines-May-target-testing-capacity-COVID-19.html
13. See: https://news.abs-cbn.com/news/05/28/20/highest-recorded-number-of-coronavirus-covid19-cases-update-doh-as-of-may-28
14. See: https://newsinfo.inquirer.net/1282501/doh-records-539-covid-19-cases-highest-spike-in-a-day
15. See: https://verafiles.org/articles/vera-files-fact-sheet-what-you-need-know-about-senates-anti
16. See: https://www.esquiremag.ph/politics/news/nbi-summons-citizen-who-made-unlawful-utterances-online-a00293-20200402
17. See: https://newsinfo.inquirer.net/1274533/nbi-summons-mocha-uson-for-posting-fake-photo-of-ppe-donation

18. See: https://www.rappler.com/nation/261251-duterte-federalism-campaign-goes-online-coronavirus-pandemic

19. See: https://news.abs-cbn.com/news/05/03/20/calida-warns-ntc-against-issuing-provisional-authority-to-abs-cbn-affiliates

20. See: https://www.rappler.com/nation/263790-maria-ressa-reynaldo-santos-jr-convicted-cyber-libel-case-june-15-2020

Vino Lucero is a project and communications officer at EngageMedia in Manila. Before joining EngageMedia, he contributed to the Philippine Center for Investigative Journalism.


POLAND
POLICING
QUARANTINE

VIA APP

Magdalena Brewczyńska

The quarantine obligation and abundance of enforcement measures

The coronavirus pandemic is posing a difficult test for many of the world's democracies, but countries such as Poland, where since 2015 the rule of law has been under threat, may be at a higher risk of crossing a critical red line.

This dispatch aims at addressing some concerns regarding the way in which certain civil liberties were curtailed in Poland in the name of halting COVID-19. More specifically, it will focus on technology-led measures for the enforcement of quarantine obligations, which invite multiple questions on their legality, necessity, and proportionality in a democratic society.

Compared to most other European countries, Poland had almost six extra weeks to prepare for the outbreak of the coronavirus. To anticipate the upcoming events, already on March 2, 2020, the first emergency bill ('The COVID-19 Act')[1] was adopted. Soon after the first positive diagnosis of COVID-19 was confirmed, various 'corona laws' (not necessarily all backed by the Parliament, but often in the form of executive orders) started to be announced, reaching a total number of 129 by mid-June.[2] In this difficult-to-navigate maze of newly adopted, amended, and annulled provisions, numerous far-reaching measures significantly affecting fundamental rights and freedoms (including the right to privacy and data protection) were introduced.

1

2

One of the measures that Poland has taken very seriously is quarantine. The existing Act of 2008 on preventing and combating infectious diseases[3] allows for the quarantine of persons exposed to an infectious disease or persons who were in contact with a source of the biological pathogen.[4]

3

4

In addition to this, on March 13, 2020, the Polish Minister of the Interior and Administration issued an executive order closing the borders for the foreigners and obliging citizens returning to Poland to undergo a 14-day quarantine.[5] Shortly thereafter, the obligation was extended to also include all household members of a person in quarantine.[6] Such a broadly defined personal scope of the quarantine obligation led to an exponential growth in the number of people subject to this measure, and consequently difficulties arose in verifying their compliance with the imposed restrictions. The capacities of the police, who traditionally used to regularly visit the addresses of people in quarantine and request them to look out the window, started to be insufficient. This, in turn, gave rise to the idea of employing a technological solution.

Poland adopted three measures involving technology in the context of monitoring people in quarantine. The most unique concerns a mobile application called 'Home Quarantine', the use of which upon the revision of the COVID-19 Act became a legal obligation applicable to everyone in quarantine.[7] Interestingly, before the app was made compulsory, the government tried to encourage citizens to use it by proposing a choice: 'either receive unexpected visits from the police, or download this app'.[8] The app prompts users to share their location data and send selfies on request in order to prove that they are staying put.[9] Through the use of facial recognition technology and analysis of location information, the state has attempted to enforce the law via the app. Remarkably, the app's privacy policy[10] fails to indicate law enforcement as a purpose of data processing and claims that the processing takes place for the protection of public health.[11] Furthermore, it provides for a surprisingly long data retention period, namely six years, with the exception of the pictures, which are supposedly deleted after the end of the 14-day quarantine period. This, together with the fact that the app's database is accessible to several entities (including the police) for the entire data retention period, makes it difficult to disregard the fears of function creep and potential abuses.

The other two measures adopted to monitor people in quarantine involve direct access by the state to location data. First, the prime minister gained a competence to issue an administrative decision that may require the telecommunication service provider to share with provincial governors and other local bodies information about the location of the devices of users on whom containment measures have been imposed. Due to the extraordinary context, such a decision did not allow for an appeal and did not require justification.[12] The lack of transparency is amplified by the fact that neither the government's requests for individual location data, nor responses thereto, are shared with the public.

Second, through an amendment made to the Telecommunication Act,[13] the Minister of Digital Affairs was attributed a right to gain access to the location data of infected and quarantined persons from telecommunication service providers.[14] Besides being questionable from a legal standpoint,[15] the way of introducing such an intrusive exception to the principle of confidentiality of telecommunication data (including location data) is very worrisome from the perspective of the legislative drafting process. The provision creating the new competence was smuggled into an act known as 'Anti-Crisis Shield 2.0.',[16] the main purpose of which was to create stimulus measures for the economy harmed as a result of the coronavirus.

Tough restrictions without pronouncing the state of emergency

The above concerns regarding the measures adopted in Poland should not overshadow the broader constitutional picture, and more specifically the fact that all the 'corona laws' were adopted without a formal declaration of the state of emergency. The reason to refrain from recalling Chapter XI ('extraordinary measures') of the Polish Constitution,[17] which contains rules for 'switching the country into a special legal regime meant to overcome exceptional dangers'[18] seems to have been influenced by the 2020 presidential election.[19]

Whilst, during the state of emergency, the introduction of certain restrictions of rights and freedoms enshrined in the

constitution may be permissible, without declaring such
20 a state, only the general derogation clause can apply.[20] Accordingly, any limitation must be 'imposed only by statute, and only when necessary in a democratic state for the protection of (...) health (...), or the freedoms and rights of other persons (...) [and] shall not violate the essence of
21 freedoms and rights.'[21] Yet, the mere fact that many of the measures, including the compulsory quarantine upon arrival from abroad, were introduced by means of executive orders (i.e. lower-level legislation and not statutes) brings their constitutionality into serious doubt.

The way forward

At the time of writing in mid-June 2020, when the epidemic curve appears to have been flattening across most of Western Europe, Poland is still experiencing a linear progression of the epidemic. Despite this, almost all lockdown measures have been removed, as the presidential election is just around the corner. The quarantine obligation applies to substantially fewer people, but the measures of its enforcement remain unchanged.

Regrettably, not much attention seems to be given in the public debate to these legally dubious measures described in this contribution, and the potential threats they may entail. This is disappointing, considering how often the call for the restoration of the rule of law is being repeated in the ongoing presidential campaign. It is hard to imagine that in a democratic state ruled by a constitution and a respect for fundamental rights, any extraordinary powers gained during a pandemic would be anything other than temporary.

References

1. See: http://prawo.sejm.gov.pl/isap.nsf/download.xsp/WDU20200000374/O/D20200374.pdf

2. This is the number of legal acts found with the search engine of the *Journal of Laws* on June 17, 2020, that referred in their scope to the term 'COVID-19'. See: http://dziennikustaw.gov.pl/szukaj

3. See: http://prawo.sejm.gov.pl/isap.nsf/download.xsp/WDU20082341570/U/D20081570Lj.pdf

4. Art. 2 indent 12 of the Act of 2008.

5. See: http://prawo.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20200000434

6. See: http://prawo.sejm.gov.pl/isap.nsf/download.xsp/WDU20200000658/O/D20200658.pdf

7. See Art. 7e of the COVID-19 Act as amended on March 31, 2020, Dz.U. item 567: http://prawo.sejm.gov.pl/isap.nsf/download.xsp/WDU20200000374/U/D20200374Lj.pdf

8. Though many cases have been reported of police checking people's presence in the traditional manner, despite use of the app. See: https://www.abc.net.au/news/2020-04-25/coronavirus-poland-tracking-quarantine-selfie-app/12173884

9. For more on the functioning of the app, see: https://www.cbsnews.com/news/coronavirus-update-poland-quarantine-app-asks-selfies-to-prove-isolation-social-distancing-police-patients

10. The privacy policy exists as one, rather short, paragraph in the app's terms and conditions, see: https://www.gov.pl/attachment/0e28593f-46f3-4460-9b3c-a00b909ffb18

11. For analysis of the problem of the purpose of processing and the choice of the legal basis, see: Brewczyńska, M. (2020) Report: The Polish Government's Actions to Fight Covid-19: A Critical Look at the 'Selfie App' and Direct Access to Location Data. *European Data Protection Law Review* 6 (2): 301-307. DOI: https://doi.org/10.21552/edpl/2020/2/17

12. See: https://panoptykon.org/pandemia-lokalizacja

13. See: http://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20041711800 as amended

14. Art. 11f. See: http://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20200000695

15. The compliance of the derogation introduced into the Polish Telecommunication Act with the exception provided for in Art. 15 of the e-Privacy Directive (Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) [2002] OJ L 201/37) seems problematic. One reason being the lack of reference to the protection of 'public health' in the catalogue of purposes that may justify interference with the general rule.

16. See: http://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20200000695/O/D20200695.pdf

17. The Constitution of the Republic of Poland of 2 April 1997 [1997] Dz.U. No 78 item 483.

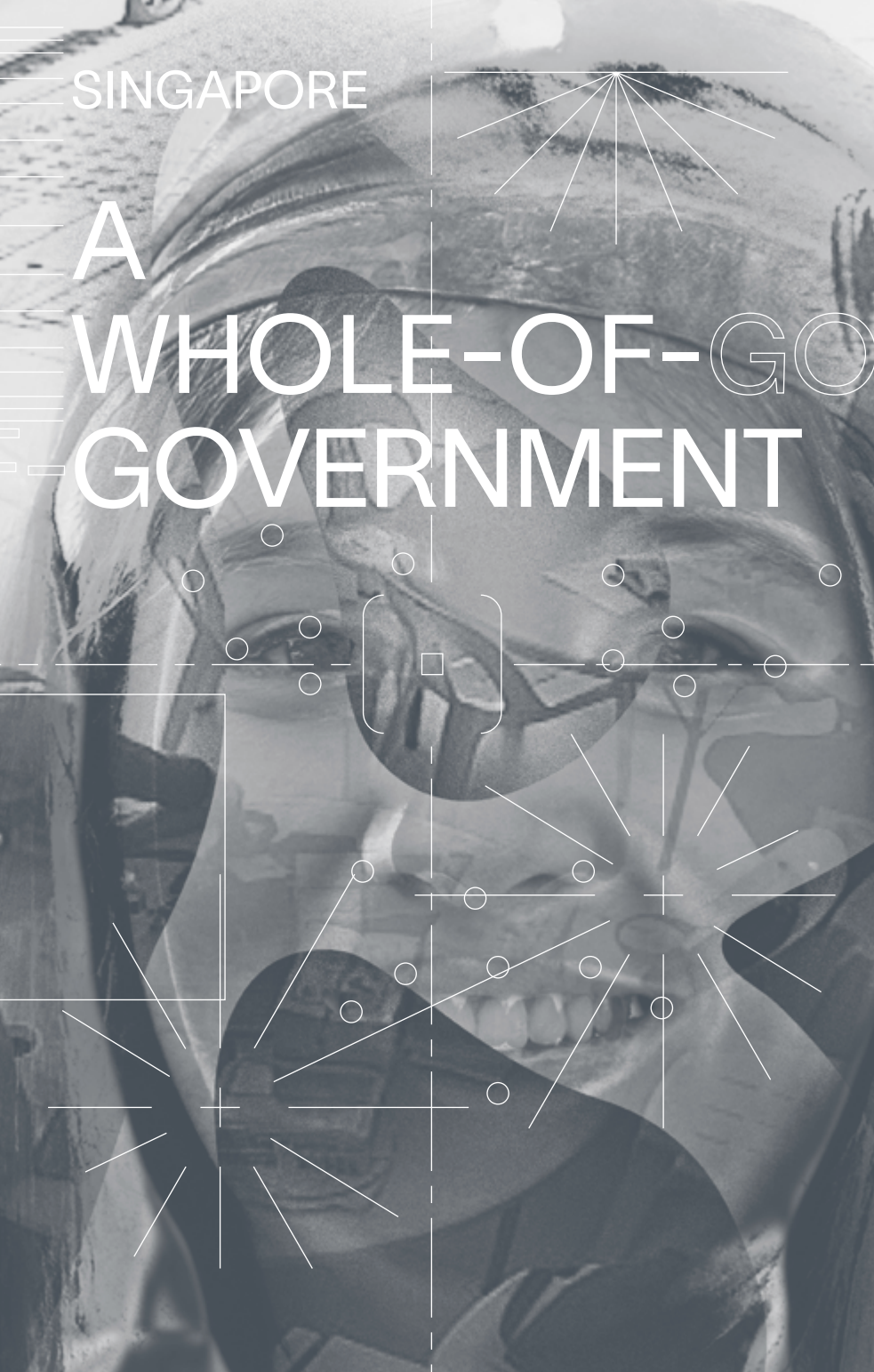
18. See: https://verfassungsblog.de/an-emergency-by-any-other-name-measures-against-the-covid-19-pandemic-in-poland

19. The coronavirus outbreak hit Poland amid a presidential campaign. The election was originally scheduled for May 10, 2020, and subsequently rescheduled to June 28, 2020. The declaration of the state of emergency would result in further delay, given that according to Art. 228 par. 7 of the constitution, during a period of introduction of extraordinary measures, as well as within 90 days following its termination, elections for the presidency cannot be held. Furthermore, during a period of introduction of extraordinary measures the Act on Elections to the Presidency must not be subject to change. In light of the dynamics of the situation, increasing fatigue with the lockdown measures, and increasingly uncomfortable questions regarding the management of the crisis, Poland's ruling party Law and Justice (PiS), which supports re-election of the current President Andrzej Duda, has repeatedly refused to declare the state of emergency.

20. Art. 31 of the constitution.

21. Art. 31 par. 3 of the constitution.

Magdalena Brewczyńska is a PhD researcher at the Department of Law, Technology, Markets, and Society at Tilburg University in the Netherlands.


SINGAPORE
A
WHOLE-OF-GO
GOVERNMENT

APPROACH TO THE PANDEMIC

Julienne Chen and Ate Poorthuis

In January 2020, when the first publicly reported signs of COVID-19 began to emerge in China, the Singapore government was quick to respond with preventative measures for its residents to follow. The government's response has been informed by a number of factors including its earlier experience with SARS and its efforts over the past several years to strengthen digital capabilities, both within government agencies and amongst the general public. It also builds upon an intensive pre-existing effort to develop and adopt technology to become a 'smart nation'. In this short piece, we focus on just a few areas in which data and technology have played a key role in Singapore's response.

Singapore's relationship with technology

Singapore is one of the most digital societies in the world. 98% of households have Internet access and 89% of individuals aged seven and above are Internet users. The mobile penetration rate, or the number of mobile (smart) phone subscriptions divided by the total population of Singapore, is more than 150%.[1] Cashless payments and e-payments have become widespread in part due to strong support by the government. These ongoing efforts to create a digital society have been an important foundation for much of the government's technological responses to COVID-19.

1

Reporting on infections

Like many nations, the Singapore government has issued a daily press release and situation report highlighting
2 the number of new cases.[2] The release of information is synchronised with the media and a number of social media channels including Facebook, Twitter, and Telegram. One key platform for dissemination is WhatsApp, which is the most widely used chat application in Singapore. Close to
3 20% of the population[3] subscribes to regular WhatsApp updates on the number of new cases, as well as general information and reminders on safe distancing.

At the beginning of the pandemic, detailed information was made publicly available about individuals who had tested positive for COVID-19—including residence block, gender, age, ethnicity, citizenship, place of work, links to other known
4 cases, and the hospital in which they were warded.[4] Over time, and as the number of cases has increased, there has been a decrease in the detail made available about these individuals. As of the end of April 2020, the information being provided on a daily basis has been pared down to age, gender, and nationality. More detailed information is provided only about individuals who work in the public healthcare sector. In the daily reports, a key distinction is also made between 'cases in the community' (i.e., Singaporeans, Permanent Residents, and Work Pass holders) and 'Work Permit holders', which primarily refers to low-wage migrant workers, most of whom live in employer-provided dormitories. Work Permit holders have been the most susceptible to testing positive for COVID-19, representing 89% of all cases in Singapore
5 as of May 9, 2020.[5]

Contact tracing

Singapore's contact tracing consists of a multiple step process. First, the hospital interviews the patient to create an activity map of the previous 14 days. This activity map is sent to the Ministry of Health, which oversees contact tracing and employs teams to verify each activity map within 24 hours. They use CCTV, data analysis, interviews,

and field teams to identify close contacts. The Singapore Police Force also provides support in finding unreachable or unfindable contacts.[6]

As the COVID-19 pandemic has unfolded, Singapore has leveraged its existing institutional capacity to create a set of additional technologies to aid in contact tracing. Key to this effort is GovTech, Singapore's technology agency, whose software development capabilities allow the government to build new technologies without needing to rely on external, commercial vendors.

One example is TraceTogether, a government-developed application that people are encouraged to install on their mobile phones. TraceTogether uses Bluetooth to identify other nearby phones that have the TraceTogether app installed. If someone becomes infected, the data can be used to identify those with whom the person was in close proximity. The app does not track an individual's location and stores and shares data under a specific set of opt-in conditions. Its implementation is open-source and published in a white paper,[7] and its relatively quick roll-out has contributed to an ongoing international discussion about the efficacy of measuring social distance through Bluetooth. Usage of TraceTogether is voluntary, and, as of the end of April 2020, only approximately 20% of the population had installed it.[8] A lower-tech wearable dongle is being explored as an alternative for those who do not have a smartphone.

Similarly, GovTech developed SafeEntry, a mobile phone-based system to log building visitors. Use of SafeEntry is required for all businesses and services, with employees and visitors using a QR code to check in and out of the premises using their name, identity number, and mobile phone number. This data forms an integral part of opening up the country after the initial lock-down, and is used for contact tracing and (in aggregated form) analytics.[9] Alternatively, people may scan their national ID card for access to publicly accessible buildings, although some retailers require the use of SafeEntry via smartphone.

Community policing

The community-at-large has been an important player in ensuring compliance with safe distancing measures. There are a number of official and media channels, pre-dating COVID-19, which residents use to bring attention to violations of rules and social norms. This type of community policing can have a strong effect in a small city state where people are easily identifiable, and it is common for images and videos of such violations to spread across multiple media channels.

For instance, the Straits Times, the newspaper of record in Singapore, has an online portal called STOMP. The portal allows people to submit photos or videos accompanied by a short caption. Many submissions are of individuals conducting 'anti-social' activity, often including their faces and other identifiable information. Numerous examples of people not adhering to COVID-19 regulations have gone viral in these and other media, with their images and personal information such as name, citizenship and ethnicity subsequently being widely publicised. Many cases are subsequently investigated by the police and brought to court where fines and jail sentences are given for infractions. Court cases are regularly reported by the Straits Times, featuring a detailed write-up of the infractions as well as a gallery of photos taken near the courthouse that show the faces of those who were prosecuted that day.[10]

Citizen reporting also happens through official channels. OneService App is the government's existing mobile phone app for residents to report municipal issues and to make service requests. Shortly after the spread of COVID-19, the app was updated with a 'Safe Distancing' category, and people were actively encouraged to use the app to take a photo and report people not adhering to the rules (e.g., not wearing a mask or loitering).[11] The information is used to identify hotspots where people are not complying with safe distancing measures, which could then result in stepped up enforcement activity in those areas.

These on-the-ground efforts are also supplemented with technologies such as drones[12] and a recent trial of a four-legged robot hound,[13] which use aerial photography and

cameras equipped with video analytic software, respectively, to monitor visitor density in public spaces such as parks. This information is subsequently fed into several online platforms where residents can check how crowded places are before they go there. The government agencies have stated that such cameras do not track and / or recognise individuals or collect personal data.[14]

Media and disinformation

In October 2019, the Singapore government passed a fake news law called the Protection from Online Falsehoods and Manipulation Act, commonly referred to as POFMA. POFMA gives the government the right to require false information that has been posted on the Internet to be taken down or to be amended with a visible correction notice. This law applies to individuals as well as the companies that facilitate the posting of such information, such as Google, Facebook, and Twitter. POFMA has been used numerous times to correct posts about COVID-19, such as reports about infection numbers inconsistent with the government figures, or claims about specific government actions or inactions.[15] The government's strict approach towards disinformation has not only quelled false information that is widely shared and forwarded amongst individuals, but also arguably has had an impact on public discourse, including concerns raised by local activists about Singapore's response to COVID-19.[16]

One of the defining features of Singapore's COVID-19 response is the extent to which it has been shaped by the pre-existing institutional capacity in terms of both governance and technology. The government was able to quickly leverage its technology agency—GovTech—to create a series of apps and platforms to help with different aspects of the response. For instance, government-developed technology was used to ensure compliance with different lock-down regulations, such as wearing of masks at all times. In doing so, the government was able to manage the response with a great level of control, at the same time iteratively rolling out new features to respond to the changing situation.

The government's continuous and pre-emptive work to create the organizational structure, tools and infrastructure

to swiftly take control in emergency situations is apparent. Long-standing efforts to encourage a 'smart nation' with high digital adoption by its citizens has allowed the government to take a decidedly technological approach in its COVID-19 response. Existing efforts to drive adoption of the government's OneService were leveraged to aide citizens to report infractions. Similarly, the fake news law—passed several months before the pandemic—became an effective tool to curb the spread of misinformation about the situation.

Conversely, the public debate in Singapore has revolved largely around the government's regulations and infractions thereof, with less emphasis on critical discussion of the specific lock-down and opening-up procedures that have characterized debates in many other countries. Further, the outbreak of COVID-19 infections amongst Singapore's population of low-wage migrant workers—often attributed to their living and working environments—show that an ostensibly well-oiled institutional and technological response also faces limits, and must constantly be re-evaluated in the broader social context within which it operates.

References

1. See: https://www.imda.gov.sg/infocomm-media-landscape/research-and-statistics/infocomm-usage-households-and-individuals

2. See: https://www.moh.gov.sg/covid-19

3. See: https://www.mci.gov.sg/pressroom/news-and-stories/pressroom/2020/4/gov-sg-launches-new-channels-to-keep-the-public-informed-about-covid-19

4. This has given rise to various dashboards such as https://againstcovid19.com/singapore/ dashboard used by citizens to keep informed, but also to avoid areas perceived as being high risk.

5. See: https://covidsitrep.moh.gov.sg

6. See: https://www.straitstimes.com/multimedia/a-guide-to-singapores-covid-19-contact-tracing-system

7. See: https://bluetrace.io/static/bluetrace_whitepaper-938063656596c104632def383eb33b3c.pdf

8. See: https://www.straitstimes.com/singapore/more-need-to-use-contact-tracing-app-for-it-to-be-effective

9. See: https://safeentry.zendesk.com/hc/en-us/articles/900000700203-Does-the-Government-have-access-to-the-data-What-will-the-data-be-used-for

10. See: https://www.straitstimes.com/singapore/courts-crime/coronavirus-woman-who-provided-sexual-services-among-5-people-sentenced-over

11. See: https://www.gov.sg/article/covid-19-resources

12. See: https://www.straitstimes.com/singapore/environment/nparks-using-drones-to-monitor-number-of-visitors-in-nature-areas

13. See: https://www.straitstimes.com/singapore/robot-reminds-visitors-about-safe-distancing-measures-in-bishan-ang-mo-kio-park

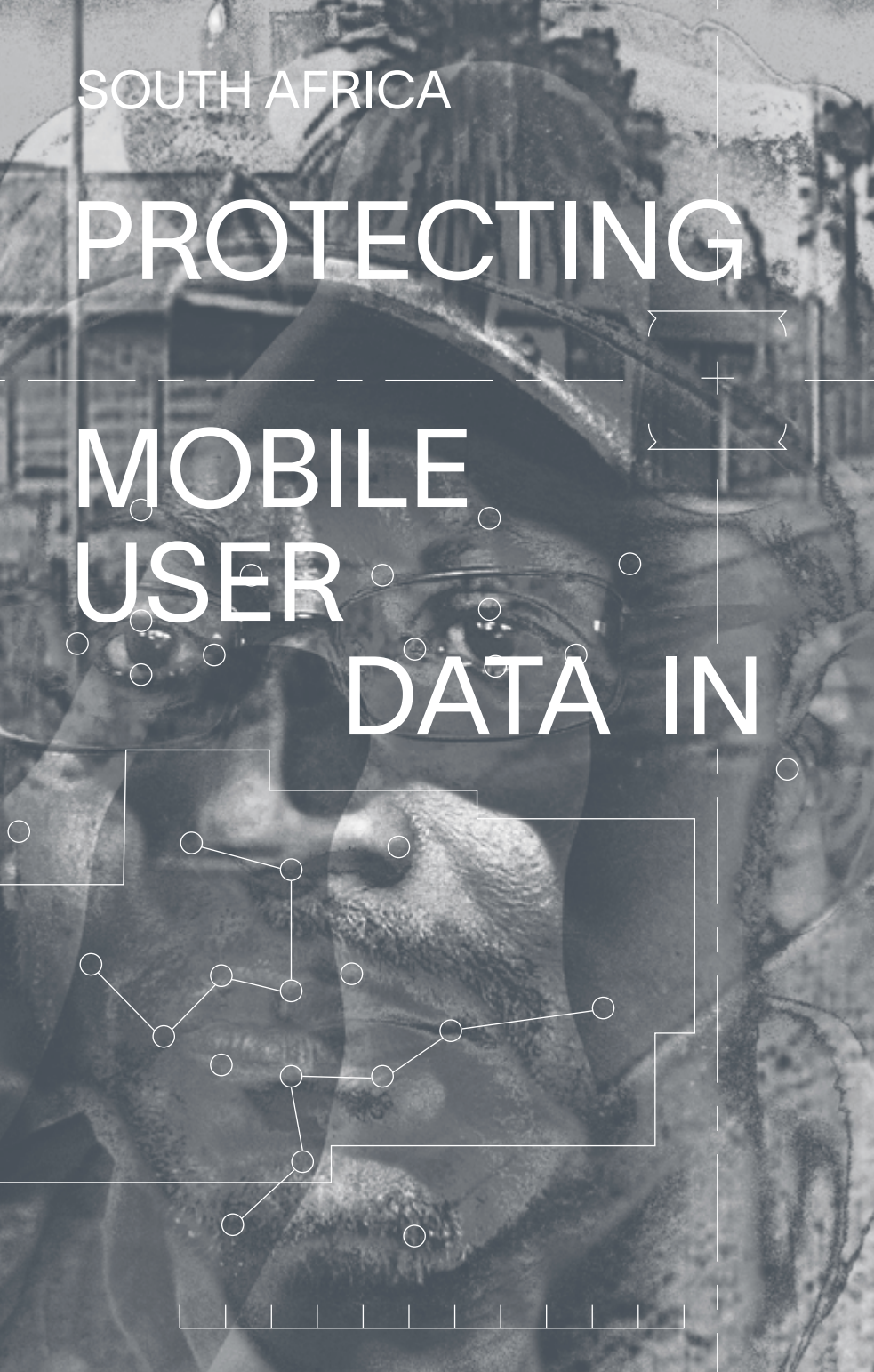
14. See: https://www.tech.gov.sg/media/media-releases/spot-robot-trial-for-safe-distancing-operations

15. See: https://www.gov.sg/pofma?type=Factually

16. See: https://www.washingtonpost.com/news/powerpost/paloma/the-technology-202/2019/12/02/the-technology-202-facebook-issues-disclaimer-demanded-by-singapore-government/5de3faf188e0fa652bbbdafa

Julienne Chen is a research fellow at the Lee Kuan Yew Centre for Innovative Cities at the Singapore University of Technology and Design.

Ate Poorthuis is an assistant professor (geography) at Singapore University of Technology and Design.


SOUTH AFRICA
PROTECTING
MOBILE
USER
DATA IN

CONTACT TRACING

Alison Gillwald, Gabriella Razzano,
Andrew Rens, and Anri van der Spuy
Research ICT Africa

A time of crisis presents an important opportunity for both asserting existing rights protections, but also for learning about the priorities of state actors in different jurisdictions in terms of their relationship to data. In South Africa, one of the earliest acts in the formation of regulations in response to the pandemic was to expand the state's powers for data extraction from citizens: even with some safeguards for rights, questions remain as to whether this extraction has adequately protected the privacy rights of citizens.

Initially it looked as if things were heading in the direction of unqualified and arguably unconstitutional mass surveillance when on March 26, 2020 at the start of the lockdown, the Communications and Digital Technologies Minister issued a set of 'directions' which included an instruction to mobile operators to provide mobile data as required by the public sector to manage COVID-19, with no limitations on the purpose of data collection or who could access the data within the public sector—or in fact, any reference to data protection at all.

The 'directions' seemed inconsistent with the Bill of Rights which remains in full force because the government declared a state of disaster to deal with the pandemic, rather than a state of emergency which would have allowed for the suspension of rights. These concerns were swiftly quelled

by an amendment to the regulations gazetted in terms of the Disaster Management Act that require telecommunications providers to supply geolocation data to health authorities for the purposes of contact tracing only. While the legal status of the 'directions' issued by the Minister of Communications and Digital Technologies is not clear, what is clear however is that the Disaster Management Act authorises regulations including the detailed contact tracing regulations. In May 2020 media reported that the obligations on telecommunications operators to provide data to the public sector had been removed based on communication by the acting Minister of Communications and Digital Technologies on deletion of the earlier wide-ranging Ministerial 'directions'. However the disaster management contact tracing regulations, including the provisions on judicial oversight remain in force.

The regulations limit the scope of collection of mobile data by a COVID-19 tracing database to only those people who are known (or reasonably suspected) to have come into contact with anyone known (or reasonably suspected) to have already contracted the virus. The information is fed into the contact-tracing database of the Department of Health, for which the Director General of Public Health is responsible.

The regulations also ensure oversight of the process by a designated 'COVID-19 Judge', and the Minister of Justice and Correctional Service, Raymond Lamola, astutely appointed respected Former Constitutional Judge, Kate O'Regan, to monitor the collection and use of location data for the contact database.

That said, the COVID-19 regulations in question have been injected abruptly into an incomplete data protection landscape in South Africa. Although legislation on personal data protection (the Protection of Personal Information Act, or POPIA) was passed in 2013, it is not yet fully in force. Indeed, the recent data collection developments might have pitted the disempowered Information Regulator against the COVID-19 National Command Council established under the Disaster

Management Act, were it not for the novel inclusion of a designated COVID-19 Judge to oversee any data collection and storage, and to safeguard the privacy of citizens.

The Information Regulator, Pansy Tlakula, responded to the obligations placed on operators to give geolocation data to government by issuing a statement highlighting that the rights to privacy and access to information are at stake with contact tracing, but supported the undertaking of it for the purposes of containing COVID-19.[1] In addition, the regulations included some of the privacy touchstones in data collection: accountability of the collecting parties, the collection only of data required for the specific purpose and its accuracy, and limitations on the retention of data beyond the state of disaster.

The regulations make no reference to the Information Regulator or the Protection of Personal Information Act.[2] Although the act was established eight years ago, as of the time of writing significant portions—including some conditions for 'responsible parties' to lawfully process personal data—are not in force, despite the Information Regulator's direct request for the President to bring the remaining sections into force by April 1, 2020. Instead most of the provisions come into force from 1 July 2020, but anyone processing personal data has a year to comply.

The contact-tracing regulations authorise sharing and use only of location and identification data, and specify that the contents of any communication may not be intercepted by the health authorities or anyone else. The regulations also limit collection and use for the specific purpose. Data may only be collected, used, and disclosed by authorised persons for the purposes of addressing, preventing or combatting the spread of COVID-19 through the contact-tracing process for the Tracing Database. While South African law ordinarily requires a judge's order for communication interception, in the regulations this collection of individual data and request does not require such an order (though a judge, as already noted, has been assigned to oversee the process more broadly).

The regulations also require the Department of Health to keep the information 'confidential' without mentioning

security—though confidentiality might require security. And the government department responsible has been accused
3 of sharing patient data with third parties before.[3] Both the Director General DG of Health and the COVID-19 Judge are required to file weekly reports stating the number, names, and details of all persons whose location or movements were obtained. This will contribute to the oversight of collection, and may go some way to assisting in the minimisation of collection as necessary.

252 The duration of the data collection is also circumscribed and terminates with the end of the national state of disaster, thereby limiting the scope of the exercise. The regulations require that every person whose information was obtained be notified of such, within six weeks of the national state of disaster lapsing, as a nod to data subject participation. It is not clear why the regulations do not require alerting data subjects at the moment of data collection, which would be relatively easy to do through text messaging.

The regulations require that all information on the COVID-19 Tracing Database, which has not been de-identified, is destroyed once the state of disaster has ended. While de-identification is not defined in the regulations, it is defined in section 1 of POPIA. If the government were to depart from that definition in its implementation of the regulation it would be difficult to justify since a definition in legislation passed by Parliament, albeit not yet in force, would enable an interpretation of hastily drafted regulations that is more consistent with the Bill of Rights.

There is however recognition in the regulations themselves that they may require adjustment to deal with conditions on the ground in order 'to safeguard the right to privacy while ensuring the ability of the Department of Health to engage in
4 urgent and effective contact tracing.'[4] The COVID-19 Judge is enabled to propose such further amendments to the Cabinet.

Unlike many other countries, the South African use of data is solely for contact tracing and not for enforcement of movement restrictions. Yet questions remain. How useful will the location data be in contact tracing? What are the

actual mechanics of collecting and storing these data? Can they be safeguarded, particularly during the collection phase? The Judge's mandate to propose improvements to the regulations is both an acknowledgement of the temporary, contingent nature of the regulation, as well as the importance of the constitutional guarantee of privacy in South Africa. The novel appointment of a (respected) specialist jurist to safeguard constitutional rights definitely makes the South African citizens winners, though the challenges and uncertainty of implementation remain.

The Information Regulator may be a loser in the government response to COVID-19, in that this could have provided an opportunity for her to put her stamp of authority on this fundamental rights issue at a time of crisis. Despite her active guidance, with the Act not fully in force she has not really been able to do so. The Regulator's clear guidelines for data protection compliance still do not bear the force of law that the regulations do, but it will be important to see how principle-based laws such as POPIA might be used to frame data justice discussions in South Africa, even if yet not with the full force of their authority.

References

1. See: https://www.justice.gov.za/inforeg/docs/InfoRegSA-GuidanceNote-PPI-Covid19-20200403.pdf
2. See: https://www.michalsons.com/focus-areas/privacy-and-data-protection/protection-of-personal-information-act-popia
3. See: https://ewn.co.za/2019/03/11/exclusive-national-health-lab-services-accused-of-unlawfully-sharing-patient-records
4. See: https://www.gov.za/sites/default/files/gcis_document/202004/43199rg11078-gon446.pdf

Research ICT Africa is a think tank working to build the ICT policy and regulatory research capacity needed to inform effective ICT governance in Africa.


SOUTH KOREA
FIGHTING DISEASE WITH APPS:
RESHAPING RELATIONSHIPS
SHIPS BETWEEN
010-8352-1967
010-3997-2968

GOVERNMENT AND CITIZENS

Sarah H. J. Kim and Melissa H. S. Yoon

South Korea's battle against COVID-19 has centred around the government swiftly delivering accurate information through various channels including emergency text alerts, government websites, televised press conferences by the South Korea Center for Disease Control and Prevention, and mobile apps. This essay introduces the COVID-19 related mobile apps, analyses why these apps have been so popular in South Korea, and discusses their significance in reshaping the relationship between government and citizens in dealing with the virus.

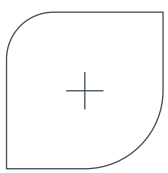
COVID-19 related apps in South Korea

Several apps have been developed to help the public deal with COVID-19. These apps generally serve as a medium that distributes information about the disease and confirmed patients, and do not collect data from individuals. They first appeared in the market in early February 2020 and the number grew rapidly.[1] These apps can be categorised by their providers and purposes. The three main providers are the government, the South Korean Medical Association, and private developers. Purposes include mask inventory apps, COVID-19 map apps, real-time status information apps, etc.

1

Government providers include the Ministry of Interior and Safety (MOIS) and the Ministry of Health and Welfare (MOHW). *Safety Didimdol*, released by the MOIS, provides disaster-related information and services.[2] The MOHW's Emergency Medical Information Provider app is a map-based app that pinpoints nearby hospitals and pharmacies, provides information on their operating hours, and shows real-time updates on bed availability in emergency departments.[3] The South Korean Medical Association has developed an app called Corona Fact – Shield to Prevent New Coronavirus, which provides real-time COVID-19 updates with push alerts.[4]

Most of the South Korean COVID-19 apps have been created by private developers, the vast majority of which provide maps with the travel histories of confirmed patients. The most popular map app is the Corona 100m, which displays government-provided travel history information in a map form and alerts users when they come within 100 metres of a location visited by a confirmed patient.[5] Similar apps include Corona Map and Corona Doctor.[6] These apps were developed by average citizens, mostly college students, rather than big-name companies. It is difficult or even impossible to identify the individual confirmed patients from the information provided by these apps. This can be attributed to several factors. First, the data used in these apps are government-provided data that have undergone the de-identification process. Second, the data released by the government is mainly focused on the locations visited by confirmed patients, rather than the patients themselves. The government-released information is limited to confirmed patients' gender, age, and residing sub-borough (or *Dong*; typically a population of around 23,000).[7] Lastly, the high population density of South Korea makes it almost impossible to identify patients just from their travel histories.



Mask inventory apps have also proved popular. In light of the mask shortage crisis, the South Korean government implemented a public mask-distribution system whose sales

points were mainly pharmacies. It also released mask sales data through an open API, which encouraged developers to create apps that notified users of the mask inventory status of pharmacies nationwide.

There were also apps that showed locations of churches and organisations of Shincheonji, a cult whose congregation sparked the first mass outbreak of COVID-19 in South Korea, with over 4,710 confirmed cases. However, since Shincheonji is discreet about its membership, the apps had to rely on information reported by people connected to Shincheonji. There have been some concerns regarding the accuracy of the information provided by these privately developed apps. For those apps that used government-provided data, this concern was only relevant in the earlier stage of the pandemic, when data was migrated manually from government sources to the apps. Now much of the government data is offered to the public through an open API, making these apps more accurate than ever. The government-supplied location data is accurate since they collect them from telecommunication and credit card com-panies directly rather than relying on public self-reporting. This collection of data is made possible under the applicable laws. However, for those apps that rely on publicly provided data, such as the Shincheonji app, concerns about accuracy remain.[8]

Currently, many of these private apps are unavailable in app stores. Following pleas by the US White House for technology companies to help stop the spread of COVID-19 misinformation and disinformation online, Apple and Google have banned all COVID-19 related apps developed by unofficial sources.

Why were COVID-19 related apps popular in South Korea?
Two important questions we should ask about the South Korean COVID-19 related apps are why were they preferred to websites and broadcasting, and why privately developed apps were more popular than government ones.

Apps were favoured over websites and broadcasting mainly because mobile apps made finding information more

convenient. Seeing the travel histories of confirmed patients on a map app is easier than reading a list of locations posted on a government website. Moreover, South Korea has the necessary infrastructure, digital literacy, and a culture that favours apps.[9] Lastly and most importantly, South Korea is one of the few countries that has been fighting COVID-19 only through social distancing policy rather than a physical lockdown. South Korea has been employing an epidemiological approach, where the government expends resource on gathering the travel histories of confirmed patients and testing anyone who came into contact with them. People are not forced to be in isolation. Instead, the government has asked the public to voluntarily practice social distancing. Thus, this pandemic has intensified the existing propensity for South Koreans to obtain information fast and in a format that enables them to stay safe while carrying out their daily lives.

The reason for the popularity of the privately developed apps can mostly be attributed to the absence of appropriate government apps. The available government apps were designed for general disaster situations, rather than COVID-19 specifically. Moreover, these apps are not particularly user-friendly, given they generally just redirect the user to official government COVID-19 websites. Also, the detailed information on confirmed patients is provided by the local government, such as the borough (*Gu*). Normally, a person's area of activity spans multiple boroughs and provinces, so using the government app to avoid infected places would mean having to access multiple websites to get the needed information. In contrast, the privately developed apps, which aggregate all the government information, conveniently present the required information in real time.

Significance of the COVID-19 apps from the perspectives of power, government, and citizens

The privately developed COVID-19 apps appear to have been successful as a means to satisfy the citizen's right to know in a more accessible way. The South Korean government's response to the spread of the Middle Eastern Respiratory Syndrome (MERS) in 2015 was met with much criticism for its inadequate disclosure of information on

confirmed patients, which led to further spread of infection.[10] In response, the Infectious Disease Control and Prevention Act was amended in 2015 and again in 2020 to give the government the authority to disclose relevant information during infectious disease emergencies.[11] This may appear as if the government is simply acting as a Big Brother, but in fact reflects the importance of the citizen's right to know—a fundamental right enshrined in the South Korean Constitution. The government is now able to provide the travel histories and quarantine status of confirmed patients, and as a result, an effective information sharing system has become a key measure to prevent and control the spread of the virus.

10

11

Unfortunately, the government's information delivery system is not the most accessible, but this shortcoming was resolved by the privately developed COVID-19 apps, forming a partnership-like relationship between government and citizens. This form of public–private partnership is imperative during emergencies like COVID-19, since it can distribute responsibility for fighting the disease between the government and citizens. In South Korea, this was achieved partly by the apps, which contributed to the successful implementation of the government's social distancing policy and other preventive measures.

There are of course risks associated with this kind of information distribution process, including the issue of privacy infringement of confirmed patients, and indirect secondary damage issues such as defamation and the social stigma facilitated by the media—as well as the social stigma resulting from the public's own inferences drawn from released information. Furthermore, administrative investigation followed by potential administrative sanctions can also be conducted in order to gather more personal information on people of interest, which may lead to violations of the Data Protection Law. The distribution of responsibilities based on the sharing of necessary information among interested parties is essential when effectively managing risks like COVID-19. However, this management must take place within cautionary boundaries set to protect the legitimate interests of citizens.

References

1. According to search results on the Google Play store, there were six COVID-19 related apps on February 5, rising to 58 by March 4—a 10-fold increase within a single month.

2. These services include shelter searches, directories for emegency medical centres, fire stations and police stations, and general safety guides.

3. The Ministry of Health and Welfare also has a Self-Check Mobile App that all people traveling to the Republic of Korea (including South Koreans) are requested to install. Once a person downloads the app and registers, they are assigned a public official who will monitor the GPS signal to make sure they remain isolated at home. While this is also a COVID-19 related app, it is designed to monitor only those who were tested for COVID-19 during their two-week isolation period. This app is irrelevant to our discussion, because it is not intended for general public use.

4. Its dashboard provides up to date information on the number of tested, confirmed, quarantined, and released patients. The app also presents travel histories of the confirmed patients, foreign news, and general information on COVID-19.

5. Corona 100m was the only privately owned app with more than 2,000,000 downloads.

6. Corona Map, with over 100,000 downloads, is another map app that displays the travel histories of confirmed patients. Corona Doctor, the only privately developed app to be recommended by Google Store as a 'COVID-19 Related Information App' also provides a map with the travel histories of confirmed patients, along with other information such as locations of testing centres and hospitals, general information about COVID-19, and latest news. A unique feature of this app is the discussion forum, which allows users to share information about COVID-19 anonymously.

7. This is the average population of sub-boroughs (*Dong*) of Seoul in 2019.

8. The app listed over 700 organisations including churches and charities to be Shincheonji affiliated, but many of these were found to be false information. The app developer recently upgraded the app to only list the 1,100 addresses released by Shincheonji directly.

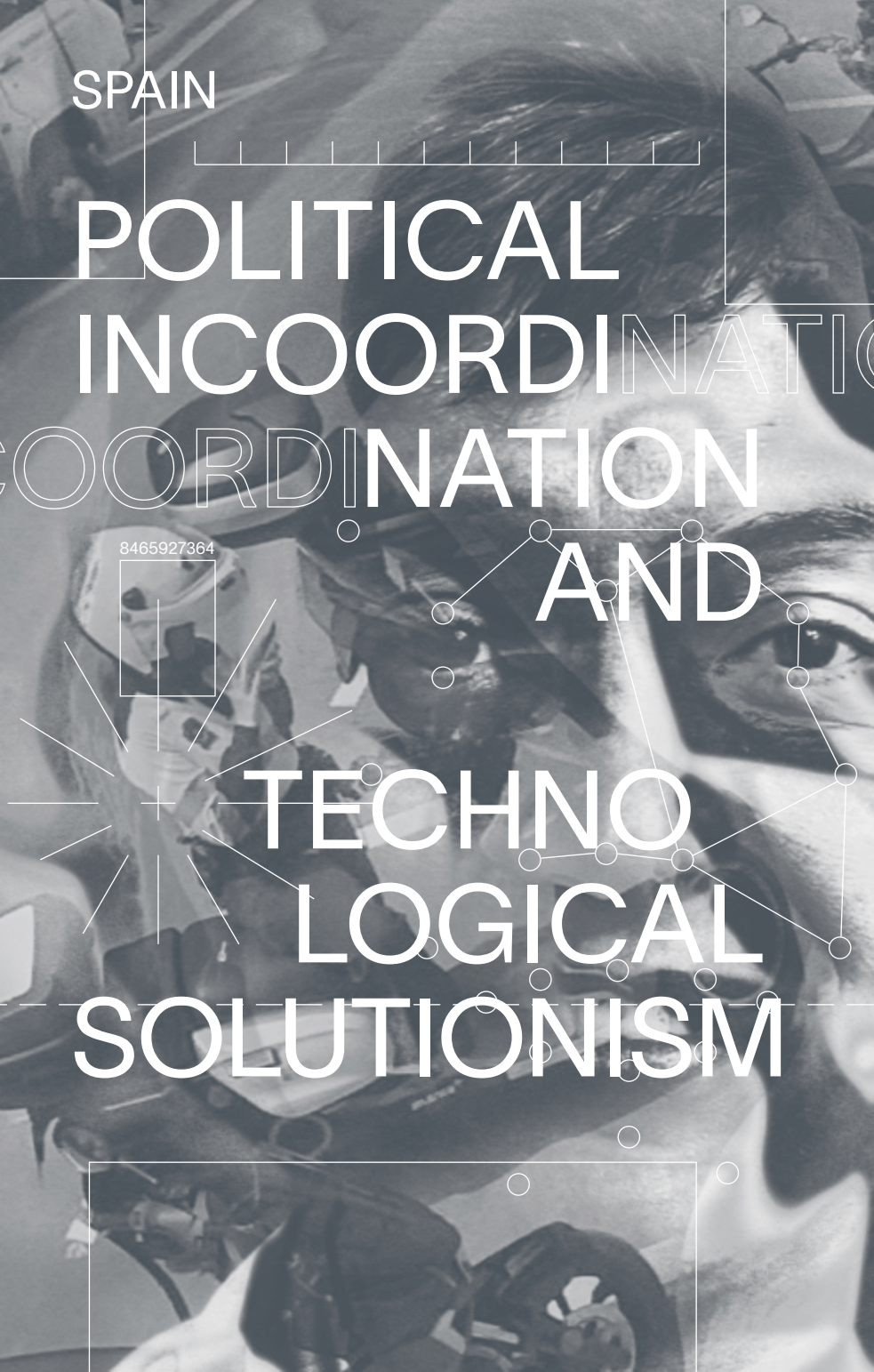
9. South Korea has one of the highest smartphone penetration rates in the world, where people of all ages use smartphones daily. Over 95% of the South Korean population uses the Internet, and the country has one of the fastest average Internet connection speeds in the world. South Korea has consistently ranked first or second in the UN ICT Development Index since the index's launch.

10. The applicable laws at the time did not allow the government to disclose or provide information they had gathered on infected patients. This led to one of the largest hospitals in South Korea unwittingly becoming one of the major points of transmission for the MERS virus. This experience revealed the need for information disclosure, especially regarding the travel histories of confirmed patients, when dealing with a crisis brought about by an infectious disease.

11. For instance, Article 34-2 of the Infectious Disease Control and Prevention Act states, 'When an infectious disease harmful to citizens' health is spreading, the Minister of Health and Welfare shall promptly disclose information with which citizens are required to be acquainted for preventing the infectious disease, such as the movement paths, transportation means, medical treatment institutions, and contacts of patients of the infectious disease: Provided, That any relevant party with respect to whom there exist any matters inconsistent with the facts among the disclosed matters or who has any opinion on the disclosed matters, may file an objection with the Minister of Health and Welfare.'

Sarah Hye Jung Kim is a recent graduate of Hanyang University School of Law in Seoul, South Korea.

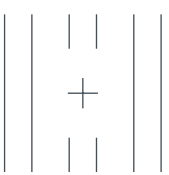
Melissa Hye-Shun Yoon is a professor at Hanyang University School of Law in Seoul, South Korea.


SPAIN
POLITICAL
INCOORDINATION
AND
TECHNO
LOGICAL
SOLUTIONISM
8465927364

AMIDST THE LACK OF TESTS

Liliana Arroyo and Enric Luján

The Spanish response to the pandemic is an example of techno-solutionism in action, fostered by time pressure and the lack of access to reliable tests. In this dispatch, we outline the main aspects of the historical and political characteristics which may explain the role of technology in Spanish health policies and how the development and deployment of apps during lockdown have been a tool for political reputation. We also highlight relevant aspects about the structure of the Spanish population and the digital penetration rates in the country, which reveal the edges of the digital divide.



On March 13, the Government of Spain declared a state of alarm over COVID-19, after counting 4,209 cases of the virus and registering 120 deaths. This state, provided in Article 116.2 of the Spanish Constitution,[1] allows the government to severely restrict the movement of people and goods, as well as most commercial activity. The day after the announcement, the decree was made public on the Spanish Official State Gazette (BOE),[2] tackling in its Article 12 the recentralisation of the Spanish national health services as long as the state of alarm lasted. The decree also gave the Ministry of Health full control over the strategy to be taken on the health front, despite the fact that after the 1978

1

2

Constitution, most health responsibilities were transferred to the 19 regional governments (representing 17 autonomous communities and two autonomous cities).

Therefore, the Ministry of Health did not have many legal powers until the decree published on March 14, which involved a recentralisation of the whole health strategy. Briefly speaking, the current situation in Spain is one where the Ministry of Health, with limited competences in health issues, has been setting the agenda of how and when to tackle COVID-19 at the national level. In turn, the regional governments, which are normally in charge of their own health services, must adapt the general plans of the ministry for their own territories, in most cases duplicating the
3 invested efforts.[3] The political incoordination resulting from this recentralisation effort is creating discomfort among the autonomous communities, while the guidelines provided by the Ministry of Health have been criticised several times for being vague and belated. Two examples help to illustrate this: the casualties database, and the seroprevalence study.

A single COVID-19 casualties database for the whole country has never existed. Every region counts their daily virus casualties and transmits the data to the Ministry of Health, which holds a daily press conference where the total numbers (infected and casualties) are updated. There are at least two limitations with this: (1) There was no unified
4 methodology for counting deaths until April 17[4] and every
5 region followed its own criteria,[5] and (2) the Ministry of Health fully relies on the updates of the regional governments, so during the weekends the number of casualties reported could be abnormally low (fewer staff, slower processing)
 and the number rises on Mondays.

After six weeks of lockdown, the Ministry of Health launched a
6 seroprevalence study,[6] with the aim of improving the capacity to assess infection levels. The National Statistics Institute selected a random sample of 36,000 households (totalling 90,000 people). The study was voluntary and included a blood test, a serology test, and a survey about symptoms for every participant. However, whilst this study was fostered by the Ministry of Health, it was carried out at the regional level, under

the responsibility of primary care centres in each autonomous community. After the first wave in May, results showed that the Spanish overall figure was five percent.[7] This is in line with studies in other European countries.

Technology as a response

Despite the process of recentralisation of health policy to tackle the crisis, it has not led to a single grand digital strategy led by the Spanish Ministry of Health to technologically mitigate the spread of coronavirus within the country. Instead, we have seen uneven regional responses based on the experience, capacity, and innovation opportunities of each territory. What follows is an overview of the responses, which rely mainly on digital technologies at two levels: apps, and population monitoring.

Official COVID-19 applications

Several official apps[8] are currently operating in Spain simultaneously, as the result of isolated responses by a number of regional governments, which either developed their own app (including Madrid, Catalunya, the Basque Country, and others) or added new coronavirus-related functionalities to their already existing regional health apps (Andalucía, Valencia, and others). Not all the apps were released on the same day or week: some regions, such as Madrid (March 23) or Catalunya (March 18) published their applications in the days following the enactment of the state of alarm.

Besides, the idea of developing a single application for the whole country has never been considered: The so-called 'national' COVID-19 application was launched on April 5, through the Department for Digitalisation and Artificial Intelligence, and it was only meant for the regions that had not developed their own (Asturias, the Canary Islands, Extremadura, and others), and had similar features.

Originally, the aim of the apps was to reduce the number of calls to the emergency services, so almost all of them offer self-assessment tools. However, some regional governments (Catalunya and the Basque Country) have also announced their plans to use them as an important source of information in the process of de-escalation—including information on the

spread of possible COVID-19 cases, evolution of infection on the ground, etc.—which is why some of the applications ask for location permissions. The Catalan app, for instance, is mobile only and monitors the GPS of its users, aiming to
9 create a patient map.[9] Catalunya is offering another map using official open data provided by the regional department
10 based on a daily registry.[10] The national app is both mobile and web-based.

It is also important to consider the fast development of the regional applications as a possible tool for political marketing (a communication exercise that appears to, but doesn't actually, solve a problem), especially when these apps have yet to play a role in the regional de-escalation response. This could likely be the case for Madrid and Catalunya, as their regional governments compete directly with the national government.

Mobility tracking and contact tracing

The Spanish National Statistics Institute (INE) has launched a study with the major telecommunications companies to analyse the mobility of the population by tracking their mobile devices. This might be considered a supplementary strategy to retain some data even if people fail to download the official COVID-19 apps. Furthermore, it might be a way of accelerating the transmission of data without the involvement of the autonomous communities. This way the national authorities can obtain some knowledge regarding the number of people that still engage in activities far from home, and also check the evolution of infection following the implementation of new measures. Despite the data being anonymised and aggregated, some privacy concerns were echoed in the
266 mass media after its announcement.[11] In parallel, by mid-
11 April the Department of Digitalisation and AI announced their commitment to the Pan-European Privacy-Preserving
12 Proximity Tracing (PEPP-PT) project, based on Bluetooth.[12]

Challenges and limitations for developing digital responses

As mentioned, the so-called technological strategy that the Spanish government has put forward is more reactive than coordinated, and despite the recentralisation of power during the state of alarm, uneven responses across the different

autonomous communities have been a constant. Despite a techno-solutionist approach operating more as political marketing, there are at least three challenges to bear in mind for any digital strategy relating to the pandemic and beyond.

The first is the digital divide, which has two important dimensions. First, 10% of the Spanish population is still disconnected;[13] mostly in rural areas, where infrastructure is costly. The population is highly concentrated in a few urban areas, while the rural areas are experiencing a steady depopulation.

13

Second, having access to the internet is not the same as enjoying quality use. The population's digital literacy is variable and heavily dependent on the level of education and cultural capital. Age is another important dimension to consider when measuring digital skills and capacities, and Spain's demographics present a particularly aged structure, with around a fifth of the population aged 65 or older.[14]

14

Last but not least, it is important to understand the privacy concerns of those who have access and are digitally literate, but who care about the management of their personal information. While the national Data Protection Authority has encouraged the development of apps and other digital solutions for data gathering,[15] trust in the government's handling of personal data for data-driven policy-making is weak. In fact, about 40% of the population is against personal data sharing to tackle the pandemic.[16] Even if a coordinated strategy existed and the national app had been deployed, the public administration is not yet considered to be a trustworthy data processor.

15

16

References

1. See: http://www.congreso.es/portal/page/portal/Congreso/Congreso/Hist_Normas/Norm/const_espa_texto_ingles_0.pdf

2. See: https://www.boe.es/diario_boe/txt.php?id=BOE-A-2020-3692

3. See: https://www.publico.es/public/budo-desconfinament-provincial-no-respon-criteris-sanitaris-funcionals.html

4. See: https://www.boe.es/boe/dias/2020/04/17/pdfs/BOE-A-2020-4493.pdf

5. See: https://elpais.com/sociedad/2020-04-15/cataluna-cambia-la-forma-de-contar-casos-y-hace-aflorar-3242-fallecidos-mas-con-coronavirus.html

6. See: https://www.lamoncloa.gob.es/lang/en/gobierno/news/Paginas/2020/20200422seroprevalence.aspx

7. See: https://english.elpais.com/society/2020-05-14/antibody-study-shows-just-5-of-spaniards-have-contracted-the-coronavirus.html

8. Most of them are apps with the purpose of self-evaluation of symptoms. At the time of writing in mid-June, while many European countries are on course to, or have already developed, contact-tracing apps, in Spain there are no plans to do so.

9. See: https://aquas-gencat.carto.com/u/aquas-gencat-admin/builder/9396196e-da82-4850-a85c-7f24b3e82388/embed

10. See: http://aquas.gencat.cat/ca/actualitat/ultimes-dades-coronavirus/mapa-per-municipis

11. See: https://www.lavanguardia.com/tecnologia/20200410/48402692952/geolocalizacion-coronavirus-datos-app-medidas-boe.html

12. See: https://www.reuters.com/article/us-health-coronavirus-europe-tech-idUSKBN21Z2AR

13. See: https://wearesocial.com/es/digital-2020-espana

14. See: https://www.ine.es/jaxiT3/Tabla.htm?t=31304

15. See: https://www.aepd.es/es/prensa-y-comunicacion/notas-de-prensa/aepd-apps-webs-autoevaluacion-coronavirus-privacidad

16. See: https://www.elperiodico.com/es/sociedad/20200426/encuesta-gesop-coronavirus-cambio-habitos-7941180

17. See: https://www.esade.edu/itemsweb/wi/research/iis/publicacions/2019_Antenna_My%20Data%20My%20Rules.pdf

Liliana Arroyo is a lecturer and researcher at ESADE in Barcelona. She coordinated the report 'My Data, My Rules: from data extractivism to digital empowerment.'

Enric Luján is PhD candidate at the University of Barcelona in Barcelona, Spain.


UGANDA
GUERRILLA ANTICS,
ANTI-SOCIAL MEDIA,

AND THE WAR ON THE PANDEMIC

Daniel Mwesigwa

President Yoweri Kaguta Museveni has been at the centre of Uganda's fight against the novel coronavirus disease (COVID-19). Just as he has been at the centre of almost every major event—and scandal—of the last 34 years. Having ascended to power in January 1986, following a five-year guerrilla war campaign imputed to a rigged 1980 presidential poll, he has overseen massive shifts in global and regional geopolitics, pandemics, and crises; as well as technology. Although the tides of time have changed the world significantly since then, the president's approaches have remained centrally rooted in guerrilla antics. The war on COVID-19, as he put it, should be treated with a 'wait and see' strategy, guerrilla style.[1]

1

Since the first case was reported in Uganda on March 21, 2020, the president has taken to the media, both traditional and new, to steer the country through regular updates and lectures characterised by long bush war stories and hackneyed military speak. Remarkably, the president has in less than two months addressed the nation more than 14 times on the pandemic and the way forward. More than before, the president, renowned for his disdain for social media as a hub of lies and falsehoods, has immensely benefited from social media—despite the social media tax (payable by social media users), which he ordered in 2018.[2]

2

In fact, in April, his Facebook following grew by 26% at an engagement rate of nearly 785%, topping popular African
3 leaders on social media.[3] Indeed, in some ways it was hard to tell whether he had become a fitness or food vlogger, having made short videos demonstrating how to work out from home and, tastefully, how to ration *posho*, a form of cooked maize meal, common amongst low income groups. It seemed the president was enjoying every bit of his reinvigorated fame and real-time influence despite being basically out of touch with the reality of ordinary citizens.

At the time of writing in June 2020, Uganda had 686 reported
4 cases.[4] Compared to other countries in the region, the number is reasonably low. Uganda's leadership has attributed this success to decisively and quickly swinging into action to close all border ports, shut down the economy, and introduce mass testing in disease hotspots—consistent to the strategy; 'wait and see.' The Washington Post has even praised the president for building on his previous successes in the early handling
272 of infectious diseases such as HIV and Ebola, and decisively handling the current
5 pandemic better than President Trump.[5] But as the nearly three-month lockdown started to take its toll on the largely peasant economy, and plans to open the economy were underway, infections started to rise fast. Truck drivers transporting cargo from Kenyan and Tanzanian seaports to Uganda, and through to neighbouring countries such as Rwanda, South Sudan, and the Democratic Republic of the Congo, were spotlighted as the unwitting vectors of the coronavirus. Nearly 95% of the newest cases
6 in May emerged from truck drivers and their contacts.[6]

Although there has been public demand to radically manage truck drivers, the president has swung in to say that stopping trucks from entering the country 'would be suicidal'; and rightly so. He added that since Uganda imports essential medical and petroleum supplies, cargo should not be blocked because "they do not come by post office or email". But he also emphasized that "you cannot tell me to leave our guns," given the country also imports raw materials like plastics for making
7 defence weapons.[7] The management of the pandemic has

not been grounded in law *per se*, bar the standard operating procedures from the Public Health Act. In fact, contrary to best practice, the president abstained from declaring a state of emergency—something that legal experts say promotes the president's individualized response over more transparent institutional action and cooperation processes enabled by the constitution for such critical moments.[8]

In some cases, the president's televised addresses have been more confusing than enlightening given the many proclamations made seemingly on the spur of the moment. The interpretation of the president's speeches by security agencies has been catastrophic. Citizens have been arrested, beaten, and in some cases killed. These include journalists doing their job and patients seeking urgent medical attention during the evening curfew hours.

On April 3, a presidential adviser coordinating the COVID-19 response announced that 'intensive surveillance' would be undertaken with the aid of mobile operators to trace more than 2,000 Ugandan individuals. Disturbingly, most information about the government's location surveillance programmes is ad hoc and dispersed across departments and agencies that may not even have the remit to conduct such sensitive duties.[9] For example, the Uganda Revenue Authority (whose mandate is to enforce tax compliance) launched a system in 2017 to track goods under customs control from point of loading to a final destination within Kenya, Rwanda, and Uganda, which has been used to monitor truck drivers for COVID-19, as was revealed on social media.[10] It became apparent the revenue body was now running a full-scale digital surveillance apparatus, due in part to the absence of strict regulation on data governance. The country's law on privacy and data protection was passed in 2019, but the attitude toward enforcement by individuals and organisations remains lacklustre.

While the president is quick enough to use crude tools from his Leninist-Marxist guerrilla past and our digital present to suppress movement and commerce—as if to suggest that that is all that's needed to contain the virus—COVID-19 has exposed Uganda's structural deficits, and the

struggles of ordinary folk not privileged enough to practice social distancing. In fact, COVID-19's compressional and accelerationist effect has seen the president's powers skyrocket. His security docket took the lion's share of the Uganda shillings (UGX) 932.7 billion (USD 250.7 million) supplementary budget allocated to fighting COVID-19, with UGX 400 billion (USD 105.7 million) reportedly earmarked for classified defence spending. The frontline fighters, the Ministry of Health, received UGX 104 billion (USD 27.4 million).[11] At the same time, the pandemic has also increased the powers of those purportedly, and surreptitiously, fighting the virus, including the revenue body and telecom companies, all of who are devouring unprecedented amounts of user data. Everything comes. Everything goes. Where to, Uganda? Let's wait for the next presidential address, perhaps.

11

References

1. See: https://www.monitor.co.ug/OpEd/Commentary/Is-Gen-Museveni-military-approach-Covid-19-workable/689364-5562340-o42vh8/index.html

2. See: https://cipesa.org/2020/05/ugandas-social-media-tax-undermining-covid-19-fight

3. See: https://www.monitor.co.ug/News/National/Covid-19-Museveni-tops-African-leaders-Facebook-follower-growth/688334-5534970-jl03uhz/index.html

4. See: https://covid19.gou.go.ug

5. See: https://www.washingtonpost.com/outlook/2020/05/01/africa-united-states-coronavirus

6. See: https://covid19.gou.go.ug/ and https://twitter.com/MinofHealthUG

7. See: https://twitter.com/jkkarungi/status/1262452983041646593

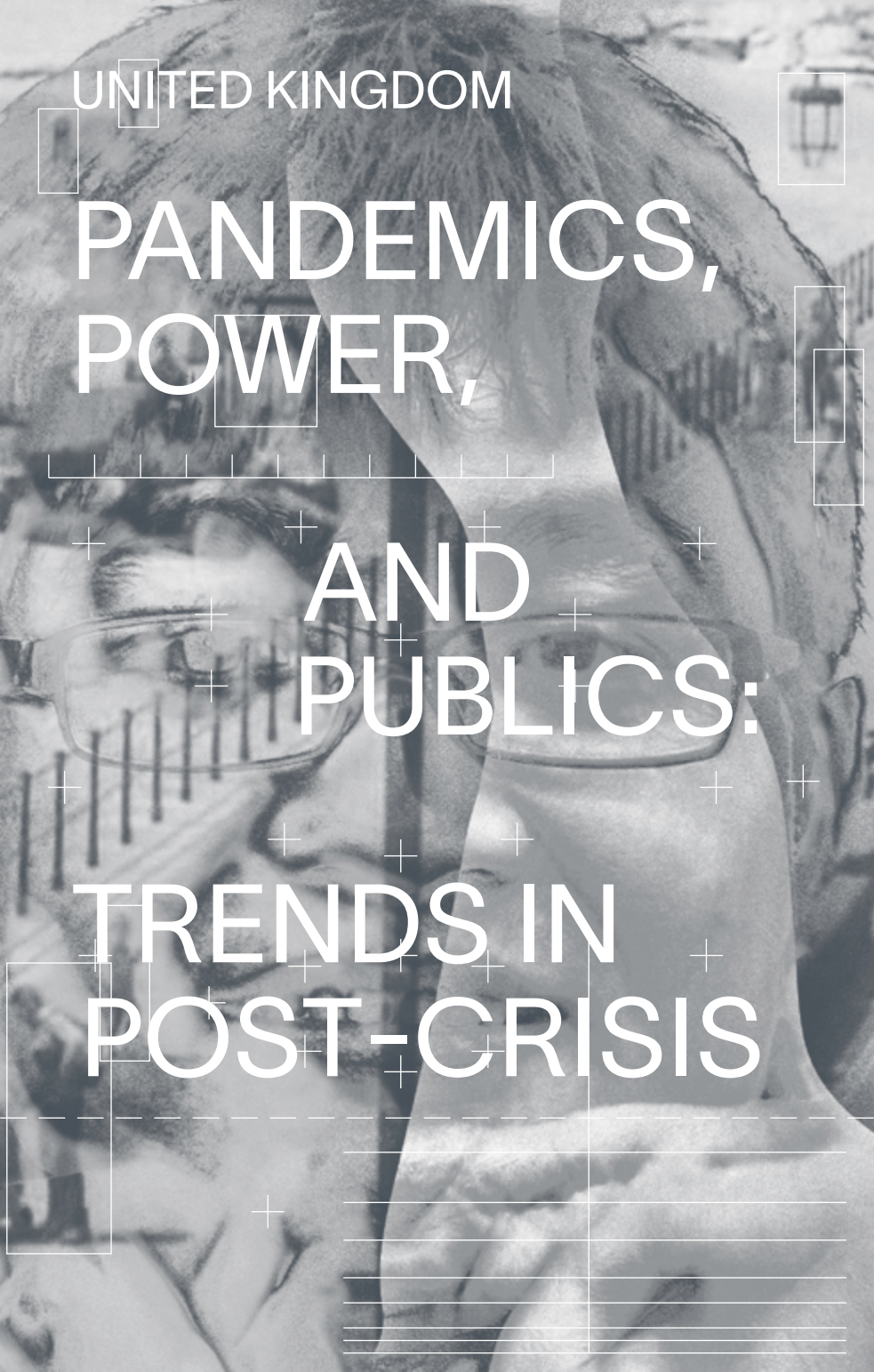
8. See: https://lawafrica.com/wp-content/uploads/2020/04/The-1995-Constitution-and-Covid-19-by-Dr.-Busingye-Kabumba.pdf

9. See: https://cipesa.org/2020/04/cipesa-submission-to-un-special-rapporteur-spotlights-rights-concerns-in-africas-covid-19-response

10. See: https://twitter.com/URAuganda/status/1250811256153481216

11. See: https://www.monitor.co.ug/News/National/How-Shs900b-extra-budget-was-shared-/688334-5533380-6a45tez/index.html

Daniel Mwesigwa is a policy analyst and researcher at CIPESA in Uganda. He is an incoming affiliate of the Berkman Klein Center at Harvard University.



UNITED KINGDOM

PANDEMICS, POWER, AND PUBLICS: TRENDS IN POST-CRISIS

HEALTH TECHNOLOGY TECHNOLOGY

Silvia Mollicchi, Aidan Peppin,
Cansu Safak, and Tom Walker
Ada Lovelace Institute

'*The National Health Service is the closest thing the English have to a religion*'
– Nigel Lawson, British politician and journalist[1]

1

Trust, power and actors of a public health crisis

Improving public health using data and technology requires a combination of factors: technological capability; political will; collated and high-quality data; and an established healthcare delivery infrastructure. Crucially, it also requires a social license gained through public trust.

These factors are dispersed disproportionately between the NHS, private technology companies, the government, the research sector, and the public. Private companies' increasingly pivotal role in delivering the UK's digital health services, catalysed by the COVID-19 pandemic, highlights two intersecting factors: private firms' power over digital infrastructure, and the indispensable role of public trust, particularly in times of crisis.

In recent years, the UK's publicly funded National Health Service (NHS) has entered into an increasing number
2 of contracts with private technology companies.[2] As it attempts to tackle the COVID-19 pandemic, the free-at-point-of-use NHS has been entering into more of these public–private partnerships.

The NHS's efforts to develop effective data analytics and cutting-edge technologies highlight the shifting power relations at the intersection of the digital economy, the delivery of indispensable healthcare services, and the need for reliable data infrastructures. While this is an ongoing trend, the current crisis offers a unique standpoint from which to examine these power dynamics and consider how the commissioning of COVID-19 related data-intensive technologies may continue or even accelerate unfolding trajectories.

Four actors hold different forms of power in the context of private-public health tech agreements—the NHS, private firms, the scientific community and people, by which we mean all individuals using the national healthcare system—and it is necessary to look at them and their mutual interactions in turn.

The NHS

The NHS is the umbrella name for all public healthcare-related services in the UK. It includes a variety of institutions, ranging from hospital trusts and authorities governing devolved healthcare provision in the country's four devolved nations, to NHSX, a body founded in 2019 to drive digital transformation in the NHS. If properly connected, structured and governed, NHS datasets could be immensely valuable for diagnostic and therapeutic research, and for improving healthcare management. The NHS thus acts as the guardian of a precious public resource—one that industry actors covet. Polling indicates that the NHS boasts consistently higher
278 levels of public trust than comparable organisations,[3] and
3 that the public are more willing to provide their clinical data
4 to the NHS than to any private actor.[4] This public trust, as well as data relating to an entire nation's health and care, gives the NHS a significant source of power.

However, the partnerships struck by the NHS and NHSX have often failed to reflect the relative strength of their position in negotiating other organizations' access to NHS data, whether patients' data or not. A 2018 contract allowing Amazon to use NHS website content data in its voice assistants, for example, permitted the company to sell 'new products, applications, cloud-based services and/or distributed software' based on that data, and to share it with third parties.[5] The contract, permissibly worded in Amazon's favour, granted Amazon significant benefits by allowing the company to develop its Alexa platform using NHS healthcare guidance that was created using public funding.

Moreover, when public–private partnerships break down, the NHS is often exposed to a greater public backlash than the private partner. After the national data protection authority ruled in 2017 that a partnership between Alphabet subsidiary DeepMind and the NHS Royal Free Hospital had failed to comply with the UK Data Protection Act when sharing patient data, the Royal Free received the bulk of public criticism.[6]

Private firms

Private companies often use their computing and financial power to increase their contractual bargaining power with respect to the public sector. As they do so, they increase their infrastructural power and contribute to the hollowing-out of publicly governed institutions. Private firms' ability to incrementally build these resilient, infrastructural forms of dominance is visible in the partnerships established during the COVID-19 crisis, most notably with the US technology provider Palantir, whose involvement in providing a new data platform (the COVID-19 datastore) has sparked controversy.[7] For several months, the UK government failed to respond to a Freedom of Information (FOI) request for the Palantir agreement's data protection impact assessments and relevant contract,[8] and only published its contract with the company after the media organisation openDemocracy and technology justice firm Foxglove threatened to sue.[9] Despite the release of the contract, there is still a lack of clear explanation of what the partnership is for, what Palantir can or cannot do, and how much influence this private firm will have over significant public investment in

health technology infrastructure in the UK. In mid-June 2020, reports indicated that the NHS had extended Palantir's contract beyond its initial term.[10]

As well as its involvement with the NHS, Palantir has secured contracts from the UK's Ministry of Defence and the Cabinet Office in recent years, and is reportedly working with several local councils in England.[11] This is likely to lead to future contracts and increasing influence on the digital infrastructure that undergirds UK public services.

The Scientific Community

As the UK government and NHSX have raced to develop technological responses to COVID-19, they have worked closely with the UK's world-leading health research and life sciences sector.[12] Organisations like Health Data Research UK and the Academic Health Sciences Network connect researchers and health data, often in collaboration with clinical care-delivery teams on a local and national level.

These actors' power, grounded in intellectual capital, has been increased by the UK government's emphasis on 'following the science' in the COVID-19 response. Many scientists argue that there is no 'one' scientific viewpoint, and that claiming to 'follow the science' obscures the political nature of government decisions.[13] The research sector's power also partly derives from public trust, which is itself drawn from perceptions that it is independent from government—even though some advisers are also ultimately government employees. Political and public attitudes place publicly funded research actors in a powerful position where their research and voice carry significant weight in determining how to use health data, and how to design technology.[14]

People

The public themselves hold considerable power. As both patients and taxpayers, the public are the NHS's most important stakeholder. In recent years, the backlash over uses of NHS data, and a focus on patient and public engagement, has highlighted the value and importance of public voice in debates about how health data is used.[15]

Services for developing diagnostic and therapeutic programmes are likely to require anonymised clinical data,[16] while services to support hospital logistics and resource allocation are likely to use non-personal operational data such as bed usage and equipment logistics.[17] Finding public support for the first type of application is obviously riskier and harder. However, it is also discussed more openly than logistical data, and subject to regulation through the GDPR and the UK's Data Protection Act.[18]

As stakeholders in the NHS and as data subjects, the public give a social license to those who wish to engage with their health data. Their power is embodied as trust, and lies in how that trust is given, and to whom. Signalling the importance of that power, NHSX has been making considerable efforts to respond to public concerns voiced by civil society organisations around the NHS's COVID-19 contact-tracing app.

This is crucial: the British public place considerable trust in the NHS but very little trust in private companies.[19] While private actors' computing power and financial capital far outweighs that of the NHS, public trust cannot be simply bought or programmed. This is particularly the case at a time of health emergency, when effective and prompt intervention relies on the public not simply acquiescing, but accurately following advice.

Trust and power

Transparency, accountability, oversight and responsible use of data are central to earning public trust. These issues are at the heart of debates around the new deals being struck in the effort to respond to the COVID-19 crisis.[20] Public health and pandemic responses are not digital services that consumers can opt in and out of according to their level of comfort with the service provider.

The trust placed in the NHS is a product of the professionalism and dedication with which it provides care, all too often in the face of adversity. But trust in healthcare systems is also a product of necessity. When it comes to our health, we may have no choice but to trust the medical advice and care we are given.

Therein lies the current concern. Private companies' increasingly prominent role in offering data-intensive health services gives them infrastructural power. As the UK public continues to rely on the NHS for health and care, the NHS's growing dependence on private services could lead to a scenario in which it is dominated by technologies and actors that the public is unable to truly challenge.

References

1. Lawson, N. (1992) *The View from No. 11: Memoirs of a Tory Radical.* London: Bantam, p. 613.

2. See: https://www.wired.co.uk/article/google-apple-amazon-nhs-health-data For background on public-private partnerships in the UK, see: https://www.nao.org.uk/wp-content/uploads/2018/01/PFI-and-PF2.pdf

3. See: https://theodi.org/article/odi-survey-reveals-british-consumer-attitudes-to-sharing-personal-data

4. Stockdale J., Cassell J., & Ford E. (2019). 'Giving something back': A systematic review and ethical enquiry into public views on the use of patient data for research in the United Kingdom and the Republic of Ireland. *Wellcome Open Research.* 3:6.

5. See: https://www.adalovelaceinstitute.org/health-data-partnerships-adas-view

6. See: https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2017/07/royal-free-google-deepmind-trial-failed-to-comply-with-data-protection-law and https://www.theguardian.com/technology/2017/jul/03/google-deepmind-16m-patient-royal-free-deal-data-protection-act

7. See: https://healthtech.blog.gov.uk/2020/03/28/the-power-of-data-in-a-pandemic ; https://tech.newstatesman.com/coronavirus/palantir-covid19-datastore-coronavirus ; https://www.opendemocracy.net/en/we-need-urgent-answers-about-massive-nhs-covid-data-deal

8. See: https://www.opendemocracy.net/en/under-pressure-uk-government-releases-nhs-covid-data-deals-big-tech

9. See: https://www.opendemocracy.net/en/under-pressure-uk-government-releases-nhs-covid-data-deals-big-tech

10. See: https://tech.newstatesman.com/coronavirus/palantir-nhs-deal

11. See: https://tech.newstatesman.com/cloud/peter-thiel-palantir-mod-contracts-2 In north-east England, Palantir worked with Sunderland council to develop an 'Intelligence Hub' that aimed to create a 'single view' of each citizen, drawing on data from a range of databases and care points. See: https://www.doc.gold.ac.uk/~bjohn002/councilwatch/index.html

12. See: https://www.bdi.ox.ac.uk/news/controlling-coronavirus-transmission-using-a-mobile-app-to-trace-close-proximity-contacts

13. See: https://www.theguardian.com/world/2020/apr/23/scientists-criticise-uk-government-over-following-the-science

14. See: https://blog.okfn.org/2020/05/05/brits-demand-openness-from-government-in-tackling-coronavirus

15. See: https://www.bbc.co.uk/news/health-26259101; https://understandingpatientdata.org.uk/news/accountability-transparency-and-public-participation-must-be-established-third-party-use-nhs

16. See: https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2017/07/royal-free-google-deepmind-trial-failed-to-comply-with-data-protection-law

17. See: https://tech.newstatesman.com/coronavirus/palantir-covid19-datastore-coronavirus

18. See: https://ico.org.uk/about-the-ico/news-and-events/blog-four-lessons-nhs-trusts-can-learn-from-the-royal-free-case

19. See: https://understandingpatientdata.org.uk/sites/default/files/2018-08/Public%20attitudes%20key%20themes_0.pdf

20. See: https://www.adalovelaceinstitute.org/wp-content/uploads/2020/04/Ada-Lovelace-Institute-Rapid-Evidence-Review-Exit-through-the-App-Store-April-2020-2.pdf At the time of writing in June 2020, the deployment of the application has been paused after an initial trial on the Isle of Wight.

The Ada Lovelace Institute is a research and deliberative body working to ensure the benefits of data and AI are justly and equitably distributed.

UNITED STATES OF AMERICA

CAPITALISING ON

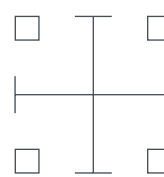
CRISIS

Julie E. Cohen

In the United States of America, across a variety of important sectors, businesses that supply networked digital information services are stepping into the gaps created by a systematic, decades-long hollowing out of public functions and competencies. Many of these developments are not entirely new; rather, they reflect the structural and infrastructural effects of long-dominant neoliberal ideologies and policies. The current crisis, however, has produced both rapid acceleration and an unprecedented scaling-up of those effects.

Internet access and multi-function connectivity

In a time of widespread (albeit varying) lockdown orders, the public have become even more deeply dependent on networked digital information services and this has underscored the effects of economic inequality on access to those services. The majority of households in 62% of US counties lack broadband Internet access, and mobile service plans in the US typically come with data caps and high overage charges.[1] The Federal Communications Commission (FCC) has urged Internet access providers to suspend data caps, waive late fees, and refrain from service cancellations during the pandemic. Many have agreed to waive fees and refrain from cancelling service, but only temporarily, and the FCC has taken no additional steps to ensure access.[2] Some members of the public have resorted to parking temporarily near libraries, cafes, and other entities that have continued to maintain publicly accessible WiFi access points.[3]



Increased dependence on networked digital information services has both intensified existing models of surveillance capitalism and created points of entry for newly institutionalised forms of surveillance. In particular,

videoconferencing platforms intensify surveillance vulnerability along a number of different dimensions. Platform purveyors typically collect large quantities of data about their users and may also store copies of intimate conversations. Zoom in particular incurred sustained public scrutiny for these reasons, but its privacy practices do not differ materially from those of other services. The rush to scapegoat Zoom has largely deflected attention from the more general default condition of inadequate privacy and data protection in the US. Meanwhile, tech giants Google and Facebook have moved to compete more aggressively in the videoconferencing space.[4] The shift to teleworking has also exposed employees and students of all ages to intensified surveillance by employers and providers of distance education services and tools—even as it has sparked calls to 'reimagine' education under the guidance of private-sector technology entrepreneurs.[5]

Countering misinformation and disinformation

The fear, uncertainty, and economic dislocation that have accompanied the pandemic have exacerbated public vulnerability to misinformation and to targeted disinformation campaigns. The business models of dominant socially networked platform companies have allowed such campaigns to flourish. Major information platform providers have taken some measures to limit misinformation about the pandemic—for example, by linking to information provided by the Centers for Disease Control and Prevention (CDC) and World Health Organization and posting warning labels on information flagged by fact-checkers—but none has done anything significant to rein in the advertiser-driven processes that target misinformation and disinformation to receptive audiences or the socially networked processes that amplify such flows.[6]

Perceiving that misinformation and disinformation work to its benefit, the incumbent administration has worked to amplify toxic information flows rather than to counteract them. The President and his closest allies have tacitly or explicitly encouraged minimisation of the health threats that the novel coronavirus presents and have worked to infuse discussion of those threats with nativism and racism.[7] Public perceptions

about the pandemic now mirror the polarisation that has characterised public opinion on so many other issues.[8] Notably, even those information platforms that purportedly have taken a more aggressive stance toward removal or restriction of pandemic-related misinformation have not extended that stance to presidential misstatements. (Twitter, the lone exception, flagged a few tweets.) So, for example, the President's speculations about the potential benefits of drinking bleach and taking hydroxychloroquine remain widely available online.[9]

Meanwhile, self-regulation remains the dominant theme in tech policy discussions both in Congress and more generally. Amidst the press of other urgent matters, momentum to enact meaningful legal restrictions on the platform business model seems to have stalled. Facebook recently founded American Edge, a DC-based lobbying organisation that will devote its resources to opposing regulation of technology interests and 'to convinc[ing] policymakers that Silicon Valley is essential to the US economy and the future of free speech.'[10]

Public health surveillance

There is widespread and growing interest in the US in proposals to harness networked digital technologies to facilitate public health surveillance, but discussions of such proposals also have highlighted the risks of misplaced faith in technological solutionism.

Public health surveillance requires comprehensiveness, competence, and public trust. Smartphone-based contact-tracing systems can generate lists that are more comprehensive than those excavated from fallible human memories, but they have other major weaknesses that concern efficacy and equity. Automated contact tracing is more likely to return false positives for members of lower income, often minority communities living or working in relatively crowded, high-contact conditions who lack the resources to self-isolate.[11] Human-centred tracing systems are better equipped to negotiate these issues in ways that encourage trust, an especially important consideration given that levels of distrust in health providers historically have been higher in such communities. In part for such reasons,

some influential jurisdictions such as New York and California have resisted proposals for smartphone-based tracing.[12]

Smartphone-based contact tracing also raises privacy and confidentiality concerns. Preliminary surveys indicate that a substantial segment of the US public would be reluctant to use smartphone-based contact-tracing tools due to fears about data leakage and mission creep.[13] Such reluctance may reflect awareness of new data-driven approaches to monitoring compliance with lockdown orders. In particular, Google has touted a 'community mobility' tool developed using aggregated geolocation data collected from users of its mobile advertising services.[14] Early contact-tracing apps commissioned by public health authorities have leaked data to mobile advertising businesses, a problem that likely reflects reliance on software developer kits supplied by those same businesses.[15] In theory, the leading proposal for smartphone-based tracing, an application programming interface (API) developed by tech giants Apple and Google, moots privacy concerns by generating nameless identifiers and storing them on users' devices rather than in a centralised database, but the proposal also reconceives public health surveillance as an opt-in activity.[16] Other reported proposals for contact tracing, moreover, involve firms that are less dominant but also substantially less reputable. Clearview AI, the controversial facial recognition start-up that built its database by scraping images from the Web and that has been linked to ultra-right-wing activists, has reportedly been in talks with several federal agencies about repurposing its system for contact tracing.[17] Private-sector employers have also shown considerable interest in smartphone-based contact tracing for their employees; so far, little information is available publicly about the means they plan to use.[18]

Manufacturing and distributing essential goods and supplies

Last but not least, the pandemic has strained supply chains for physical goods and supplies. Under crisis conditions—and against a background of federal government incompetence, indifference, and corruption—tech giant Amazon has rapidly expanded its empire, positioning itself to emerge as the dominant supplier of consumer goods in a post-crisis environment in which many brick-and-mortar businesses

will not reopen. Meanwhile, the Trump administration has retained the powerful and secretive data company Palantir to develop a health care tracking and forecasting platform, and has ordered health providers to provide Palantir with daily updates on their inventories of essential medical supplies.[19] 19

Unlike competitors such as package delivery services Fedex and UPS and the grocery shopping service Instacart, Amazon uniquely operates its own private infrastructure covering every aspect of sourcing, routing, and last-mile delivery of goods. Particularly in major urban and suburban areas, Amazon now supplies people sheltering in their homes with everything from groceries to personal care supplies to supplies and equipment for teleworking. Its decisions about sourcing and distribution therefore have vast policy ramifications. Early in the pandemic, Amazon's platform-based structure facilitated hoarding and profiteering on high-demand items.[20] Additionally, the rapidly intensifying public demand for home delivery of essential supplies tested even Amazon's formidable logistical capabilities. Amazon responded to these disruptions in ways calculated to position itself as the emergency supplier of first and last resort. Its expanded suite of house-branded offerings for groceries and personal care supplies, and its decision to prioritise delivering those orders, were sensible components of a centrally coordinated emergency response, but they also caused additional harm to small merchants operating on the platform and already struggling to survive.[21] 20 21

Increased public reliance on Amazon's home delivery services has also laid bare the extent to which those processes rely on the embodied, physical labour of warehouse workers and delivery drivers. Amazon has responded aggressively to worker demands for protection by rolling back its already inadequate sick leave policy, cracking down on unionisation efforts, and firing workers agitating publicly for better treatment.[22] So far, congressional efforts to address worker well-being have been stymied by the Senate and the White House, where the health and welfare of blue-collar workers newly recognised as essential have become bound up with deeply racialised stances on public health, public welfare, and the rights and privileges of citizenship.[23] 22 23

Without question, responding to the COVID-19 pandemic requires mobilizing the resources and expertise of information technology firms to provide internet access, counter misinformation and disinformation, facilitate public health surveillance, and coordinate physical supply chains. Equally without question, allowing those processes to unfold in ways superintended by the firms themselves and structured by their economic interests threatens important public values.

References

1. See: https://www.theguardian.com/world/2020/apr/13/coronavirus-covid-19-exposes-cracks-us-digital-divide

2. See: https://arstechnica.com/tech-policy/2020/03/after-deregulatory-blitz-fcc-scrambles-to-prevent-isp-abuse-during-pandemic

3. See: https://www.nytimes.com/2020/05/05/technology/parking-lots-wifi-coronavirus.html

4. See: https://www.cnn.com/2020/04/30/tech/zoom-google-facebook/index.html

5. See: https://www.vox.com/recode/2020/4/2/21195584/coronavirus-remote-work-from-home-employee-monitoring; https://www.vox.com/recode/2020/5/4/21241062/schools-cheating-proctorio-artificial-intelligence ; https://www.aclu.org/news/privacy-technology/those-free-remote-learning-apps-have-a-high-cost-your-students-privacy ; https://www.vice.com/en_us/article/pkyenm/new-york-is-turning-into-a-silicon-valley-science-experiment

6. See: https://theconversation.com/social-media-companies-are-taking-steps-to-tamp-down-coronavirus-misinformation-but-they-can-do-more-133335 and https://www.theverge.com/2020/5/12/21254184/how-plandemic-went-viral-facebook-youtube

7. See: https://www.nytimes.com/2020/04/21/us/politics/coronavirus-protests-trump.html ; https://www.americanprogress.org/issues/security/news/2020/04/14/483119/trumps-coronavirus-survival-strategy-blame-china ; https://www.theatlantic.com/ideas/archive/2020/05/americas-racial-contract-showing/611389

8. See: https://knightfoundation.org/articles/americans-struggle-to-navigate-covid-19-infodemic and https://www.forbes.com/sites/mattperez/2020/05/10/death-toll-conspiracy-why-conservative-media-and-soon-possibly-trump-are-doubting-coronavirus-mortality-figures/#520161c757d5

9. See: https://www.politico.com/news/2020/05/27/coronavirus-twitter-trump-286716 ; https://www.nytimes.com/2020/04/30/technology/trump-coronavirus-social-media.html ; https://www.theverge.com/2020/4/9/21209797/trump-chloroquine-hydroxychloroquine-medication-social-media-misinformation

10. See: https://www.washingtonpost.com/technology/2020/05/12/facebook-lobbying-american-edge

11. See: https://www.lawfareblog.com/importance-equity-contact-tracing and https://www.brookings.edu/techstream/inaccurate-and-insecure-why-contact-tracing-apps-could-be-a-disaster

12. See: https://thehill.com/opinion/technology/493648-how-human-centered-technology-can-beat-covid-19-through-contact-tracing and https://www.wired.com/story/health-officials-no-thanks-contact-tracing-tech

13. See: https://arstechnica.com/tech-policy/2020/04/half-of-americans-wont-trust-contact-tracing-apps-new-poll-finds

14. See: https://arstechnica.com/tech-policy/2020/04/half-of-americans-wont-trust-contact-tracing-apps-new-poll-finds

15. See: https://www.washingtonpost.com/technology/2020/05/21/care19-dakota-privacy-coronavirus

16. See: https://www.bloomberg.com/news/articles/2020-04-13/apple-google-covid-19-contact-tracing-to-require-verification

17. See: https://www.buzzfeednews.com/article/carolinehaskins1/senator-markey-clearview-ai-covid-contact-tracing

18. See: https://www.npr.org/2020/05/08/852896051/your-boss-may-soon-track-you-at-work-for-coronavirus-safety

19. As of this writing in June 2020, most details about the Palantir contract are still unknown. See: https://www.thedailybeast.com/fema-tells-states-to-hand-public-health-data-over-to-palantir

20. See: https://www.nytimes.com/2020/03/14/technology/coronavirus-purell-wipes-amazon-sellers.html and https://observer.com/2020/03/coronavirus-amazon-matt-colvin-hand-sanitizer-profit

21. See: https://www.wired.com/story/amazon-essential-items-policy-devastating-sellers

22. See: https://www.theverge.com/2020/4/14/21220353/amazon-covid-19-criticism-protest-fired-employees-cunningham-costa-climate-change and https://www.latimes.com/business/technology/story/2020-04-09/fearful-of-covid-19-amazon-workers-ask-for-state-probe-of-working-conditions

23. See: https://www.theatlantic.com/ideas/archive/2020/05/americas-racial-contract-showing/611389

Julie E. Cohen is Mark Claster Mamolen Professor of Law & Technology at Georgetown Law Center in Washington, DC.


WESTERN BALKANS
INSTRUMENTS
84756190
OF

CHILLING POLITICS

Bojana Kostić, Bojan Perkov, Andrej Petrovski, Danilo Krivokapić

The coronavirus pandemic has dramatically changed people's lives in the Western Balkan region. According to the Oxford COVID-19 Government Response Tracker, Serbia, North Macedonia, Croatia, Montenegro, and Kosovo have been described as countries with the strictest restriction of movement measures.[1] Introduced in mid-March,[2] these were followed by the closure of public and private venues, including public transport. In Serbia, even the parliament was suspended so the national emergency was, against the Constitution, declared by Government Decree.[3] In addition, police-enforced curfews were introduced from midday, combined with a several days-long lockdown.[4]

These restrictive measures do not come as a surprise given that most of the Western Balkan countries have witnessed a worsening of the political environment and overall lack of trust in political institutions.[5] For example, a 2020 Freedom House report found that Serbia is no longer considered a democratic state, but 'partly free' and under a 'hybrid regime'.[6] Other countries in the region, according to the same assessment, are also considered partly free or free democratic states.[7] In the same vein, the yearly EU assessment reports published by the European Commission note that in many Western Balkan countries there is little or no progress in the field of judicial independence, rule of law, and media freedom.[8]

It is against this background that—despite generally positive trends in technological development, including relatively

high Internet penetration and mobile phone use in the region,[9] relatively functional (yet fragile) e-government infrastructure,[10] and the fairly positive status of human rights online[11]—technology in the time of pandemic has been used as 'vehicles for exercising power',[12] reinforcing the negative tendencies described above.

In a nutshell, technological interventions have mainly been used as a means to chill certain forms of behaviour and further limit human rights. This is especially clear in the context of surveillance technologies across the region, which resonates with the overall concept of the 'epidemiological turn of surveillance technologies' (see introductory chapter). In addition, these interventions have lacked transparency and public debate, including the involvement of expert communities, and overall understanding of the beneficial effect of a particular technology. Firstly, there was the lack of knowledge about the use of particular technological measures and their implications. Secondly, there were often no easy-to-use redress and correction mechanisms, and one can also question their efficacy as the emergency situation also meant limitation of certain fair-trial guarantees. This is particularly true in the context of Serbia, which hosted a large number of wide-ranging Chinese experts (medical and 'techno-pandemic' experts, law enforcement and military officials) to combat the virus, which also suggested inclusion of the technological, mainly securitisation measures similar to those used in Wuhan. But, as noted, the absence of publicly available information and explanation increases the suspicion that the techno-health agenda of pandemic control was just a smokescreen to strengthen and potentially entrench restrictive environments.[13]

This case study outlines the ways in which these pre-existing hostile environments, coupled with new chilling technological tendencies, exacerbate the overall techno-societal dynamics and reinforce their associated negative potential. It is mostly based on the monitoring work of a pioneer digital rights organisation, SHARE Foundation, which has been following the situation in the region since the beginning of the pandemic.[14]

Assessment of the key technological trends during the state of emergency

Most of the examples here depict techno-societal processes that, as noted, lack basic transparency in terms of both their functionality and access to efficient redress procedures. In addition, little is known about their efficiency; at least the public was not informed about the relevance of these processes in controlling the spread of the virus. A brief legal analysis suggests that many of these technological measures are likely to be unconstitutional and do not adhere to the positive legislative framework.[15]

The pandemic situation in the Western Balkans has reconfirmed practices and policies in the context of surveillance technologies. As before, non-transparent and fear-driven attempts to introduce the use of these technologies have been recorded. For example, the President of Serbia announced that the police had been tracking movements of 'Italian phone numbers', referring to the mandatory quarantine measures for Serbian expats returning from Italy when the state of emergency was proclaimed.[16] This chilling measure should be observed in the context of the country's already problematic practices of direct access to retained communications metadata[17] stored by telcos. In that sense, this measure has increased suspicions of unlawful and arbitrary mass surveillance, without the civil and public control and accountability of the state authorities. This is further compounded by the fact that the new smart video surveillance system for Belgrade,[18] provided by Huawei and announced in early 2019, has continued to be installed during the pandemic.[19] In relation to this argument, there was an attempt in Croatia to introduce legislative changes, which would enable tracking of citizens' mobile phones, though this was later put on hold.[20] Coupled with the fact that some Croatian cities started using drones to monitor public areas for breaches of state measures, this reveals the pervasive use of surveillance technologies as well as their unpredictable effect on the life of citizens.[21]

There are also notable risks for privacy and personal data protection, especially regarding health data. In general, the following examples indicate the often reckless and

inadequate treatment of citizen data collected en masse during the pandemic. For instance, login credentials for Serbia's national COVID-19 information system were left exposed on the web page of a health facility for eight days, long enough to be indexed and become searchable on Google, according to the SHARE Foundation, which discovered the page by accident.[22] Other incidents related to health data have occurred in North Macedonia, where a list of all citizens that tested positive for COVID-19 in one city was leaked on social media;[23] in Montenegro, whose National Coordination Body for Infectious Diseases published online the names of citizens ordered to self-isolate;[24] and in Bosnia and Herzegovina, where local authorities published data about infected citizens and those in quarantine and self-isolation. At this moment it is hard to say whether data will be misused in the future, but these examples surely demonstrate the absence of awareness and respect towards citizen data held by the state.

Another adverse factor in the pandemic response was that these databases were new and created ad hoc. Thus, it is hard to understand and verify whether they are in fact compliant with the personal data protection and information security legal framework. On the other hand, North Macedonia's coronavirus tracing mobile app[25] might seem like a positive development. With the use of the app being voluntary and the data being stored on the device only for 14 days, it is based on a decentralised, endpoint-hosted data store (i.e. data stored locally on mobile devices) using Bluetooth connections for contact tracing. It appears as a much more effective and less intrusive solution, in line with the European Commission guidance on apps supporting the fight against COVID-19 pandemic in relation to data protection.[26]

Misinformation, a global phenomenon, can cause informational disorientation and decrease trust in the media, especially taking into account controversial statements from the highest public officials.[27] In Serbia, misinformation has an additional layer of concern given that media freedom has been under concerted attack for years.[28] Instead of technological means to counter this global trend, the Serbian fact-checking initiative[29] relied on journalists and researchers

to debunk swarms of unconfirmed and outright false claims since the pandemic started. The Croatian fact-checking portal has also noticed and recorded a large number of false, misleading, and unchecked information about the pandemic and the virus itself, mostly spread via social media and popular chat apps such as Viber or WhatsApp.[30] Spreading rumours and unverified information on social media has proven costly for at least one Russian citizen in Montenegro: a woman arrested for 'spreading panic' after she posted claims that 'a thousand people are infected in Montenegro and that six people died' as well as that 'Montenegro is expecting the Italian scenario'.[31] To tackle these problems and the problem of violation of self-isolation measures in Serbia, the so-called Skype trials—court proceedings conducted via video link or Skype application—were introduced. These 'turbo' criminal proceedings have often stayed hidden from the public, and conflict with the Serbian constitution and the peremptory norms of the criminal law.[32]

30

31

32

Drawing upon these examples and analyses, it may be argued that across the region technology has mainly been used as a securitisation measure and chilling instrument to ensure that citizens comply with stringent and—at least from a human rights perspective—profoundly questionable lock-down measures. In turn, the centralised and non-transparent process of decision making in the context of technological responses to COVID-19 has most likely resulted in further erosion of human rights and democracy, but perhaps also hindered the Western Balkan governments' potential to control the pandemic. Thus, the question remains open whether these measures were proportionate, legitimate, and necessary, as well as whether the state authorities will be held accountable for the excessive restrictions of human rights. However, given the overall lack of accountability and critical voices in the Western Balkan region, it is hard to expect that an open and pluralistic public debate will take place after the emergency situation is revoked and state institutions reopen.

In semi or fully authoritarian regimes the pandemic will most likely provide governments with more power to limit or violate human (digital) rights. Thus, as much as in the global context, the Western Balkan techno-societal dynamic will continue to

challenge the democratic process and potential of citizens to push for lifting these limitations so as to prevent them from becoming the new normal. This is particularly true for big data analytics and mass surveillance practices through metadata or smart video surveillance—an extremely intrusive system for the right to privacy and by proxy for other human rights, notably the right to freedom of expression and the right to freedom of association. Misinformation and lack of genuine public debate will continue to challenge the public's understanding and trust in the state's decisions and actions. Implicitly, this case study has also demonstrated that in the context of the Western Balkans there are only losers and a myriad of missed opportunities to ensure publicly beneficial use of technology to address this critical situation.

References

1. See: https://www.bsg.ox.ac.uk/research/research-projects/coronavirus-government-response-tracker ; https://www.bsg.ox.ac.uk/sites/default/files/2020-04/BSG-WP-2020-032-v5.0.pdf ; https://www.intellinews.com/balkans-have-some-of-the-world-s-strictest-anti-coronavirus-measures-179810

2. See: https://europeanwesternbalkans.com/2020/03/20/covid-19-pandemic-how-are-the-wb-countries

3. See: https://www.reuters.com/article/us-health-coronavirus-serbia/serbia-calls-state-of-emergency-to-counter-coronavirus-idUSKBN21215E

4. See: https://www.government.nl/documents/diplomatic-statements/2020/04/01/statement-by-belgium-denmark-finland-france-germany-greece-ireland-italy-luxembourg-the-netherlands-portugal-spain-sweden ; https://balkaninsight.com/2020/04/10/serbia-north-macedonia-impose-harsh-weekend-curfews ; https://www.occrp.org/en/daily/11992-serbia-s-covid-19-lockdown-takes-an-authoritarian-turn

5. See: https://doi.org/10.1080/14683857.2019.1706257 ; https://hcss.nl/report/far-right-trends-south-eastern-europe-influences-russia-croatia-serbia-and-albania

6. See: https://freedomhouse.org/country/serbia/nations-transit/2020

7. See: https://freedomhouse.org/country/montenegro/nations-transit/2020 ; https://freedomhouse.org/country/bosnia-and-herzegovina/freedom-world/2020 ; https://freedomhouse.org/country/north-macedonia/freedom-world/2020 ; https://freedomhouse.org/country/croatia/freedom-world/2020 ; https://freedomhouse.org/country/kosovo/freedom-world/2020

8. See for example: https://ec.europa.eu/neighbourhood-enlargement/sites/near/files/20190529-serbia-report.pdf ; https://ec.europa.eu/neighbourhood-enlargement/sites/near/files/20190529-bosnia-and-herzegovina-analytical-report.pdf ; https://ec.europa.eu/neighbourhood-enlargement/sites/near/files/20190529-kosovo-report.pdf ; https://ec.europa.eu/neighbourhood-enlargement/sites/near/files/20190529-north-macedonia-report.pdf ; https://ec.europa.eu/neighbourhood-enlargement/sites/near/files/20190529-montenegro-report.pdf

9. See International Telecommunication Union (ITU) data on mobile-cellular subscriptions per country, available at: https://www.itu.int/en/ITU-D/Statistics/Documents/statistics/2019/Mobile_cellular_2000-2018_Dec2019.xls , and ITU data on percentage of individuals using the Internet per country, available at: https://www.itu.int/en/ITU-D/Statistics/Documents/statistics/2019/Individuals_Internet_2000-2018_Dec2019.xls

10. See Open Government Partnership data for Serbia, available at: https://www.opengovpartnership.org/members/serbia/#intro ; Croatia, available at: https://www.opengovpartnership.org/members/croatia ; North Macedonia, available at: https://www.opengovpartnership.org/members/north-macedonia ; and Montenegro, available at: https://www.opengovpartnership.org/members/montenegro

11. See: Share Monitoring: https://monitoring.bird.tools

12. Gagliardone, I. (2014) "A Country in Order": Technopolitics, Nation Building, and the Development of ICT in Ethiopia. *Information Technologies & International Development* 10(1) 3–19, at pp. 5 and 15.

13. See: https://www.theguardian.com/world/2020/apr/13/coronavirus-diplomacy-how-russia-china-and-eu-vie-to-win-over-serbia and https://foreignpolicy.com/2020/04/08/china-serbia-aleksander-vucic-xi-jinping-coronavirus

14. For a chronological overview, see: https://www.sharefoundation.info/sr/digitalna-prava-na-balkanu-gugl-pretraga-osetljivih-podataka-o-licnosti ; https://www.sharefoundation.info/sr/digitalna-prava-na-balkanu-privatnost-pacijenata-na-udaru ; https://www.sharefoundation.info/sr/digitalna-prava-pandemija-i-balkan ; see also: https://bird.tools/mapping-digital-rights-during-coronavirus-outbreak

15. These developments merit separate legal discussion.

16. See: https://globalvoices.org/2020/03/30/covid-19-pandemic-adversely-affects-digital-rights-in-the-balkans

17. See: https://labs.rs/en/invisible-infrastructures-surveillance-achitecture

18. See: https://www.sharefoundation.info/wp-content/uploads/Serbia-Video-Surveillance-Policy-brief-final.pdf

19. See: https://www.sharefoundation.info/en/hiljade-kamera-rs-community-strikes-back

20. See: http://balkans.aljazeera.net/vijesti/pracenje-mobitela-stavljeno-na-cekanje

21. See: https://glashrvatske.hrt.hr/en/news/domestic/vukovar-police-using-drones-to-enforce-social-distancing-measures

22. See: https://www.sharefoundation.info/en/a-password-pandemic

23. See: https://sdk.mk/index.php/dopisna-mrezha/krivichna-prijava-za-objavuvane-spisotsi-so-imina-na-kumanovtsi-zaboleni-od-koronavirus

24. See: https://globalvoices.org/2020/03/30/covid-19-pandemic-adversely-affects-digital-rights-in-the-balkans

25. See: https://stop.koronavirus.gov.mk/en

26. See: https://ec.europa.eu/info/sites/info/files/5_en_act_part1_v3.pdf

27. See: http://rs.n1info.com/English/NEWS/a582547/Serbia-s-authorities-not-happy-with-Serb-nationals-returning-from-abroad.html and https://www.telegraf.rs/english/3172968-the-government-again-texts-citizens-dramatic-situation-italian-scenario-looming

28. See: https://ec.europa.eu/neighbourhood-enlargement/sites/near/files/20190529-serbia-report.pdf ; https://ec.europa.eu/neighbourhood-enlargement/sites/near/files/20180417-serbia-report.pdf ; https://ec.europa.eu/neighbourhood-enlargement/sites/near/files/pdf/key_documents/2016/20161109_report_serbia.pdf ; https://ec.europa.eu/neighbourhood-enlargement/sites/near/files/pdf/key_documents/2015/20151110_report_serbia.pdf ; https://ec.europa.eu/neighbourhood-enlargement/sites/near/files/pdf/key_documents/2014/20140108-serbia-progress-report_en.pdf ; https://cadmus.eui.eu/bitstream/handle/1814/61154/2018_Serbia_EN.pdf ; https://safejournalists.net/wp-content/uploads/2018/12/indicators_on_the_level_of_media_freedom_WB_2018.pdf

29. See: https://www.raskrikavanje.rs/covid19/?vrsta=dezinformacije

30. See: https://faktograf.hr/2020/04/28/live-blog-dezinformacije-o-koronavirusu

31. See: https://radiosarajevo.ba/vijesti/regija/pisala-na-drustvenim-mrezama-ruskinja-uhapsena-u-crnoj-gori-zbog-sirenja-panike/371329

32. See: https://engnews24h.com/serbian-bar-association-against-trial-via-skype-society

Bojana Kostić is a law and technology researcher working for a number of international organisations, originally from Serbia, currently based in The Netherlands.

Bojan Perkov is a policy researcher at SHARE Foundation in Belgrade, Serbia.

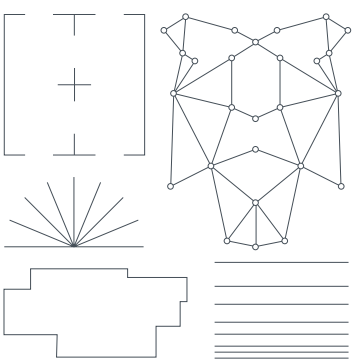
Andrej Petrovski is director of technology at SHARE Foundation in Belgrade, Serbia.

Danilo Krivokapić is director of SHARE Foundation in Belgrade, Serbia.

The design of this publication offers visual entry points to the meaning of the word surveillance. Borrowed from the French, it means literally 'to watch from above', by the combination of the prefix *sur-* ('over' or 'above') and *veiller* ('to watch', derived from the Latin verb *vigilare*, with the same meaning). This definition led to the development of a series of graphic signifiers presented across the book's layout and image-making: cartographic, monitoring, documental and tracking visual languages intertwine in overimposed layers.

Targets, trackers, flows

The layout of the publication and the images are often populated with a collection of graphic devices extracted from various monitoring technologies. These, apart from their original functional purposes—to visually manifest supposedly objective measures—entail a particular aesthetic. The visual characteristics and placement over the subjects of observation have become part of the collective imaginary. Crosses, lines, targets, trackers all form part of a visual vocabulary enforcing a fiction of accuracy.[1]



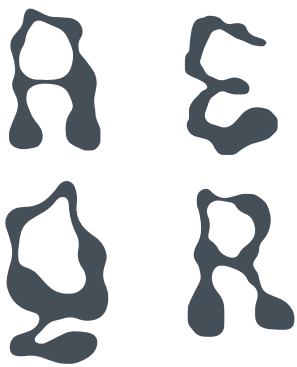
Countries and Peoples

The images at the start of each chapter in the Dispatches section offer a simultaneous read of two realities: the place and the inhabitant. The images are composed of two primary sources: site footage and facial portraits. The collection of openers explores visual manifestations for the notions of 'datalogical traces' and 'biosurveillance' presented in this volume.[2]

First, the background imagery contains snapshots taken from publicly accessible CCTV cameras. The images, apparently innocent, raise questions around the IoT (Internet of Things) of security devices. While suggesting a feeling of control by means of providing objective documentation, they are also able to expose bypassers and the life surrounding real estate.

Second, the most recognisable component of the images is a series of portraits, almost mugshots, 'imagined' with the AI-based tool *This Person Does Not Exist* by Philip Wang.[3] This tool, operated by a GAN (Generative Adversarial Network), StyleGAN2, produces 'generative data-driven unconditional' imagery.[4] The choice of AI-generated portraits questions our trust in the image as a witness of truth. In a more practical sense, it also helps avoid the use of 'real humans' in the construction of visual rhetorics.

The two layers are articulated using the typeface Quarantina by Héloïse d'Almeida, as a masking tool. The letterforms are inspired by 1960s horror movie letterings, drawing from the visual component of organic dissemination, especially in the behaviour of moulds and fungi. The choice for this typeface, developed in Paris during the 2020 Covid-19 lockdown, temporally contextualises the design of this book, emphasising how graphic designers respond to the circumstances of their context.



The elements are presented as a blend which is challenging to separate; the resulting shared surface raises questions about how publicly available information might be used. The inhabitant is subject to being monitored, while, at the same time, provides access to data and potential surveillance tools unknowingly.

'Surface, representing no particular meaning or message, is the precondition for virtual capital, projected revenue and speculative value. Advertising surface in public space initially is merely an add-on to the already existing historical structure of a city. Gradually, the surface replaces the primacy of historical structure and its territoriality. The city becomes the profit base for a virtual spin: the multiplication of surface accounts for the exponential growth of value extracted from its public space. By our being in public, by simple existence, we already automatically affirm the exposure which grants the surface infrastructure its right to the city. The inhabitants of cities are through this mechanism, directly inscribed into the means of value production.' [5]

Folios as coordinates
The layout of the folios in the Dispatches section follows a coordinate-like system. It is based on an inverted version of the Gall-Peters cartographic projection, where the north is placed along the bottom edge of the map. The running headers and footers are indicators of the longitude, while the page numbers represent the latitude.

The Gall-Peters projection is a cylindrical map projection which prioritises area representation, giving a fairer overview of land footprint when using a traditional rectangular format. This projection is the one recommended by the United Nations, as opposed to the Mercator projection, currently used in services such as Google, Apple, Baidu or Bing maps. The Mercator projection shows South America and Africa as proportionally smaller in size and has been associated with a colonial worldview.[5]

References

1. Rancière, J. (2007) *The Future of The Image*. Verso, pp. 103-107.

2. See page 58: Keyes, O. 'Who counts? Contact Tracing And The Perils Of Privacy'.

3. See: https://thispersondoesnot exist.com/

4. See: https://arxiv.org/abs/1912.04958 ; https://github.com/NVlabs/stylegan2

5. Metahaven (2008) *White Night Before a Manifesto*. Onomatopee.

6. Pater, R. (2016) *The Politics of Design: A (Not So) Global Manual for Visual Communication*. Amsterdam: BIS Publishers, pp. 152-157.

Other publications by Meatspace Press include:

Graham, M., Kitchin, R., Mattern, S., and Shaw, J. (eds). 2020. *How to Run a City Like Amazon, and Other Fables*.

Graham, M. and Shaw, J. (eds). 2017. *Towards a Fairer Gig Economy.*

Shaw, J. and Graham, M. (eds). 2017. *Our Digital Rights to the City.*

All Meatspace Press publications listed above are free to download, or can be ordered in print from meatspacepress.com

DISPATCHES

COVID-19 has reshaped how social, economic, and political power is created and exerted through technology. Through international case studies, this book analyses how technologies of monitoring infections, information, and behaviour have been applied and justified during the emergency, what their side-effects have been, and what kinds of resistance they have met.

ISBN 978 - 1 - 913824 - 00 - 6

www.meatspacepress.com