Covid-19 Apps: Policy, Legal & Technical Trends Report

Table of Contents

Executive Summary *3*
Introduction *5*
Country Background *7*
Australia 7
Bahrain 7
Chile 8
Indonesia 9
Israel 9
Netherlands 10
Tunisia 11
Western Australia 11
Global Apps 12
CommonPass 12
IATA Travel Pass 13
Covid-19: Policy, Legal & Technical Trends and Recommendations *16*
Pillar 1 - Public Health Efficacy 16
Pillar 2 - Function Creep & Unintended Consequences 25
Function Creep 25
Unintended Consequences 33
Appendixes *38*
Appendix 1: Summary of Insights and Recommendations from Phase 1 of the Covid App Project *39*
Appendix 2: Covid Apps – Key Technical Features *46*

Executive Summary

This report on Covid-19 apps and technology sets out the results from a two-phase research project on the technological response to Covid-19 around the world. Phase one covered the use of contact tracing apps in a number of countries until July 2021.[1] Phase two incorporates technological applications developed since then, most notably "immunity passports". Supported by a technical review[2] of a globally representative sample of apps, this report sets out trends in policy, legal and technical approaches around the globe. This is done through a review and technical assessment of 11 case studies of different apps developed (or commissioned) mostly by governments, but also by other actors, in Australia, Bahrain, Chile, Indonesia, Israel, the Netherlands, Tunisia, and Western Australia. These countries were selected to be representative of the different continents/regions of the world and to reflect the main trends observed during the research. The other actors developed apps with a theoretically global scope: WEF's CommonPass and IATA Travel Pass.

The report considers approaches to app design and use regarding their public health efficacy and the degree of function creep and unintended consequences for civil rights, freedoms and equal treatment. This analysis informs a set of recommendations and best practices for policymakers, tech developers and civil society to develop effective and sustainable public health practices.

The main findings of the sample case studies include:

- Launching a mobile application as a prominent part of the response to a public health emergency is unprecedented. Many countries around the world saw the launch of Covid apps, namely contact tracing apps and immunity passport apps. Both were viewed as an opportunity to take advantage of modern technology to suppress Covid-19 effectively and efficiently. Across the globe, however, the uptake of contact tracing apps by the population was low, with the vast majority of countries not managing to increase uptake beyond 25%.
- Immunity passport apps were introduced across the world, particularly when vaccines became available. Most were introduced between February and December 2021. A substantial difference in the design of contact tracing apps and immunity passports is that whereas many countries used the GAEN API as a good practice framework for contact tracing apps, no such trends were observed for immunity passports. On average, this manifests through lower privacy standards and less secure infrastructures, as well as more discriminatory surveillance resulting from both intentional and unintentional function creep.
- Across the world, there are numerous instances of large data leaks and hacks of personal public health data, and in the case of immunity passports, this led to substantial occurrences of fraud in many countries. In most cases, adhering to privacy-by-design principles could have prevented the large-scale leaking of sensitive personal data.
- While most governments and app developers did publish a privacy notice, these varied greatly in quality. None of the apps published the SDKs used in the app developments, and only three of the 11 apps examined had open-source code, namely the

[1] https://www.awo.agency/latest/covid-19-app-project/
[2] https://awo.agency/files/Covid-19-Apps-Technical-Review-2022.pdf

Netherlands' CoronaCheck app and the scanner for the CoronaCheck app and Australia's COVIDSafe.

- Some countries, such as Indonesia, made their immunity passport apps mandatory for access to society, including supermarkets, despite less than 20% of the population having received a vaccination at the time of introduction. Relying on immunity passport apps to combat the spread of Covid-19 can only function adequately if vaccines and testing are sufficiently and equitably available to the population.

Recommendations identified as part of the project include:

- Governments must ensure the development of relevant critical infrastructure for technological public health measures, and their rationale must be evidence-based to secure public health efficacy as well as fundamental rights.
- Significant uptake by the population is a key component of making technological public health measures work, and this requires both extensive public awareness and trust.
- Governments must establish permanent public procurement procedures for emergencies to prevent improper spending, corruption, and a global race to obtain limited supplies.
- Governments did not have an adequate legal framework for introducing Covid measures and apps, resulting in a state of emergency being decreed in states around the world. Going forward, a comprehensive legal framework must be established to provide the basis for emergency response public health measures.
- Governments must ensure that public health measures are not discriminatory and do not disproportionately affect marginalized groups.
- Adhere to privacy-by-design principles by only using SDKs that process the minimal amount of personal data needed for public health purposes, produce clear, user-friendly and transparent privacy notices, make the source code available to allow for independent verification of the app's purposes, and carry out data protection or privacy impact assessments.
- Anticipate attempts by both users and private sector partners to commit fraud and allow for the removal of fraudulently obtained certificates, within the privacy-by-design framework.

Technology can make a great contribution to combatting Covid-19 and potential future pandemics, but only under certain circumstances. It is not a silver bullet and must work in tandem with other evidence-based measures such as testing, vaccines, social distancing, and facemasks. As trust is key to ensuring the voluntary, large-scale adoption of contact tracing apps and immunity passports, preventing function creep and discrimination is essential not only for safeguarding fundamental rights, but also for public health efficacy.

The key findings of the combined reports are available in a toolkit,[3] tailored for use by policymakers, tech developers and civil society, which are available in eight languages: Arabic, English, Farsi, French, Hindi, Russian, Simplified Chinese and Spanish.

[3] https://awo.agency/latest/covid-app-project-phase-2

Introduction

A range of measures focused on safeguarding public health were introduced during the Covid-19 pandemic. Whilst these included traditional epidemiological measures, notably lockdowns, social distancing and quarantine mandates, technology-based measures were also put in place. Some of the most discussed interventions of this type include contact tracing apps and immunity passport apps.

Contact tracing apps are mobile apps that implement a digital version of contact tracing – the process of tracking those infected by the virus to monitor its spread and warn others of its proximity. Many countries across the world launched these apps and used digital contact tracing to complement traditional contact tracing techniques and inform the public of other measures, such as local lockdowns.

Immunity passport apps are mobile apps that allow users to show health information proving that they are unlikely to spread the Covid-19 virus. This risk is typically determined by either a person's vaccination status, a negative Covid test, or a positive antibody test showing that a person had Covid-19 previously and has some level of immunity after recovering from the virus. These apps are used to allow people to enter certain public venues or to travel to other regions or countries.

The Covid App Project is a two-part civil society initiative that stemmed from a research interest in Covid-specific interventions. Phase 1 of the project focused on contact tracing applications (hereafter "apps") in countries outside Europe and North America. Phase 1 of this shared research interest drew together six civil society organizations: ALT Advisory (South Africa), Internet Democracy Project (India), InternetLAB (Brazil), Karisma (Colombia), SMEX (Lebanon), and United for Iran. AWO, a data rights agency, provided coordination support.

During Phase 2 of the project, the research covered Covid-19 interventions since the completion of Phase 1 in July 2021. The objective is to provide recommendations regarding the use of: i) immunity passports; ii) contact tracing applications; and iii) combined features in existing contact tracing apps. Immunity passports, also known as Covid pass apps, are apps that allow users to show that they are a lower risk based on either their vaccination status, a recent negative lateral flow or PCR test, or a recovery certificate, proving that due to recent infection they are less susceptible to infection for a specified period.

The efficacy of these methods was considered from: i) a public health perspective and ii) a human rights and data protection perspective. The focus is on function creep – specifically, the use of these tools to extend social control and adversely impact social access and participation, especially by vulnerable populations, whether deliberately or not. Therefore, it assessed how apps and features were designed and deployed, and how they interacted with public health, human rights, and data protection outcomes in the following regions: Africa, the Americas, Asia, Europe, and Oceania.

More specifically, the second phase of the project focuses on a review and technical assessment of the following:

- Eleven case studies of different apps developed (or commissioned) mostly by governments, but also by a few other actors, in Australia, Bahrain, Chile, Indonesia, Israel, the Netherlands, Tunisia, and Western Australia. They were selected to be representative of the different continents/regions of the world and to reflect the main trends observed during the research.
- Two global apps: CommonPass and IATA Travel Pass.

Based on this review, the objective is to identify trends in the following areas: i) legal and policy; ii) public health efficacy of the measures deployed; and iii) risk of function or scope creep. Based on these trends, recommendations are identified and build further on recommendations identified during Phase 1 of the project. These recommendations are presented in a toolkit, which takes stock of the effectiveness and impact of Covid-19 responses, outlines the lessons to be learned from this experience, and can help improve pandemic response in the future. The recommendations focus on ways to enhance public health efficacy and to prevent function creep and unintended consequences. They also aim to strengthen public awareness of the use of Covid-19 apps.

Therefore, this toolkit is designed for stakeholders shaping public health and pandemic response: i) policy makers and legislators; ii) app developers, designers, operators and commissioning public entities. The toolkit also offers accessible information on best practices for civil society and the general public. To ensure that the toolkit is broadly accessible across the world, they are available in eight languages: Arabic, English, Farsi, French, Hindi, Russian, Simplified Chinese and Spanish.

Overall, the output of this second phase of the Covid App Project consists of the following:

- This Trend Report contains key policy, legal and technical trends in Covid-19 interventions and apps as well as recommendations. The apps and Covid-19 interventions are interpreted from two pillars: 1) public health efficacy and 2) function creep and unintended consequences.
- A report on the privacy risks of the Covid-19 apps assessed.[4] The accompanying technical report provides an extensive technical review of the 11 selected apps, considering particularly whether they adhere to best practices in data protection, including, but not limited to, privacy by design and data minimization. Accordingly, the technical report also provides recommendations for ensuring effective and safe Covid-19 apps.
- A toolkit:[5] recommendations from both the Trend and Technical Assessment Reports, as well as recommendations identified during Phase 1 of the project informs the toolkit, providing comprehensive best practices and accessible guidance for: i) policy makers and legislators; ii) app developers, designers, operators and commissioning public entities. These recommendations also provide insights on best practices for members of the public and civil society.

[4] https://awo.agency/files/Covid-19-Apps-Technical-Review-2022.pdf
[5] https://awo.agency/latest/covid-app-project-phase-2

Country Backgrounds

This section of the report sets out the relevant background to the different Covid-related apps released in our countries of focus. It also gives an overview of the features of these apps and how they have been used in the different countries.

Australia

Australia's response to Covid-19 began with national recommendations combined with localized restrictions imposed by the different states making up its federalized system.[6] However, in March 2020, the federal government, in conjunction with state authorities, agreed on more widespread restrictions on social gatherings as well as closing pubs, gyms, cinemas, restaurants, and religious establishments[7] as a result of general disregard for the original guidelines.[8] After many months of strict Covid-19 measures, which have attracted criticism in the form of protests and failed legal challenges,[9] some state authorities opted to relax restrictions in September 2021 (although others have maintained their "Covid Zero" strategy).[10]

Among the measures introduced to combat Covid-19 at the national level was the launch in April 2020 of COVIDSafe, the only contact tracing app approved by the Australian federal government.[11] At the time of its release, the Prime Minister, Scott Morrison, stated that using the app was "the ticket to ensuring that [the country] can have eased restrictions", though its use has always been voluntary.[12] Made available for iOS and Android devices, the contact tracing app was a key part of the government's Covid-19 response early on, supporting the processes implemented to identify those who have been in close contact with Covid-infected persons.[13]

Bahrain

Even before the pandemic, the Government of Bahrain had been pursuing a technology-based agenda focused on digital transformation and improving access to government services. The Information and eGovernment Authority has been central to this, with plans for the use of

---

[6] BBC. (7 April 2020). *Coronavirus: The world in lockdown in maps and charts*. Available at: https://www.bbc.com/news/world-52103747

[7] Prime Minister of Australia. (22 March 2020). *Update on Coronavirus* measures. Available at https://web.archive.org/web/20220415010336/https://www.pm.gov.au/media/update-coronavirus-measures-220320 ; Reuters. (14 March 2020). *New Zealand, Australia tighten lockdown to combat coronavirus.* Available at https://www.reuters.com/article/us-health-coronavirus-australia-idUSKBN211020

[8] Deutsche Welle. (1 April 2020). *Australia's slow reaction to the coronavirus crisis*. Available at: https://www.dw.com/en/australias-slow-reaction-to-the-coronavirus-crisis/a-52982343

[9] The Guardian. (17 August 2021). *Supreme court rejects Victorian anti-lockdown protestor's legal challenge.* Available at: https://www.theguardian.com/australia-news/2021/aug/17/supreme-court-rejects-victorian-anti-lockdown-protesters-legal-challenge; The New York Times. (20 November 2021). *Thousands Protest Covid Measures in Australia.* Available at: https://www.nytimes.com/video/world/australia/100000008086651/australia-coronavirus-restrictions-protests-melbourne-sydney.html

[10] Bloomberg. (14 September 2021). *Border Blockades Spark Australia's Biggest Crisis in 120 Years*. Available at: https://www.bloomberg.com/news/articles/2021-09-14/covid-pandemic-measures-in-australia-create-political-tension-for-scott-morrison

[11] Australian Government Department of Health. (27 April 2020). *COVIDSafe: New app to slow the spread of coronavirus.* Available at: https://www.health.gov.au/news/covidsafe-new-app-to-slow-the-spread-of-coronavirus

[12] The Guardian. (23 May 2020). *How did the Covidsafe app go from being vital to almost irrelevant?*. Available at: https://www.theguardian.com/world/2020/may/24/how-did-the-covidsafe-app-go-from-being-vital-to-almost-irrelevant

[13] Australian Government Department of Health. (ND). *How COVIDSafe works*. Available at https://www.health.gov.au/resources/apps-and-tools/covidsafe-app#how-covidsafe-works

cloud computing, blockchain and artificial intelligence to enable better access to government services through mobile applications.[14]

The advent of Covid-19 has seemingly not deterred progress on this project, as evidenced by the launch of BeAware Bahrain in March 2020. It was developed to complement efforts to mitigate the spread of the virus with its digital contact tracing functionality, thus forming part of the country's trace, test and treat strategy.[15] Eventually, being able to show a vaccine passport was added as a feature to the app, with Bahrain becoming one of the first countries to do so in February 2021.[16] It was also the first country to allow users to book a vaccine appointment through the app.[17] However, whilst built for both iOS and Android devices, the use of BeAware Bahrain has never been made mandatory for residents or foreigners.

Chile

Like the other Latin American countries, Chile struggled during the early waves of Covid-19. In April 2020, Chile reported over 10,000 cases, which was the third highest figure in the region at the time after Brazil and Peru.[18] This was also when the country opted for localized lockdowns;[19] the six million residents of Santiago, for example, saw the closure of all non-essential businesses.[20] The spread of the virus was even enough to postpone a constitutional referendum after a 90-day "state of catastrophe" was announced by President Sebastián Piñera in March 2020.[21] But it was also during the early stages of the Covid-19 pandemic that Chile proposed the idea of issuing immunity passports "to those who have overcome the disease 14 days after showing the first symptoms, and also to those who were discharged even with symptoms a week after their departure from the hospital".[22] However, plans for these immunity passports were postponed in May 2020 over fears that those without a passport may be discriminated against when applying for jobs.[23] In the end, "cases of reinfected people and an economy deeply affected by the pandemic put a stop to this program".[24]

---

[14] Alarabiya News. (13 August 2020). *Bahrain's 'BeAware' coronavirus app has saved lives: Here's how.* Available at: https://english.alarabiya.net/views/news/middle-east/2020/08/13/Bahrain-s-BeAware-coronavirus-app-has-saved-lives-Here-s-how

[15] Startup MGZN. (31 March 2020). *'BeAware Bahrain' app officially launched by iGA.* Available at: https://www.startupmgzn.com/english/news/beaware-bahrain-app-officially-launched-by-iga/

[16] Mobi Health News. (18 February 2021). *Bahrain launches digital COVID-19 'vaccine passport'.* Available at: https://www.mobihealthnews.com/news/emea/bahrain-launches-digital-covid-19-vaccine-passport

[17] Mobi Health News. (6 January 2021). *Bahrain first country to allow vaccine appointment via mobile app.* Available at: https://www.mobihealthnews.com/news/emea/bahrain-first-country-allow-vaccine-appointment-mobile-app

[18] Reuters. (19 April 2020). *Coronavirus cases in Chile top 10.000, third highest in Latin America.* Available at: https://www.reuters.com/article/health-coronavirus-chile-idUSL1N2C52HE

[19] BBC News. (7 April 2020). *Coronavirus: The world in lockdown in maps and charts.* Available at: https://www.bbc.co.uk/news/world-52103747

[20] Reuters. (19 April 2020). *Coronavirus cases in Chile top 10.000, third highest in Latin America.* Available at: https://www.reuters.com/article/health-coronavirus-chile-idUSL1N2C52HE

[21] The Guardian. (19 March 2020). *Chile moves to postpone constitutional referendum amid coronavirus crisis.* Available at: https://www.theguardian.com/world/2020/mar/19/chile-postpone-constitutional-referendum-coronavirus-crisis

[22] Infobae. (16 April 2020).*Chile entregará "pasaportes de inmunidad" a las personas que se recuperaron de COVID-19.* Available at: https://www.infobae.com/america/america-latina/2020/04/16/chile-entregara-pasaportes-de-inmunidad-a-las-personas-que-se-recuperaron-de-covid-19/

[23] Chile Today. (11 May 2020). *Chile Postpones "Immunity Passports" to avoid job discrimination.* Available at: https://chiletoday.cl/chile-postpones-immunity-passports-to-avoid-job-discrimination/

[24] Lawbrarians Monitoring covid-19. (12 December 2020). *First Steps in Chile between changes in government and immunity passports.* Availabe at:https://lawlibrariansmonitoringcovid19.com/2020/12/12/first-steps-in-chile-between-changes-in-government-and-immunity-passports/

Chile did, however, eventually release a mobility pass for fully vaccinated citizens in May 2021.[25] But before that, as an alternative to the original plans for an immunity passport, the Chilean government launched CoronApp in April 2020. This app neither performs contact tracing nor functions as an immunity or vaccine passport. However, it does have a range of other features, including the ability for users to self-diagnose based on symptoms and generate a risk classification, access information about Covid-19, report high-risk events or behaviors, and ask for or offer help to neighbors. The data collected by CoronApp allows the Ministry of Health to track those with Covid-19 or those suspected of having the virus.[26] Chileans can download the app for iOS and Android devices.

Indonesia

Early on in the pandemic, the Indonesian government was criticized for being too slow to mitigate the spread of Covid-19. It was accused of having "downplayed the pandemic's risk by ignoring warnings from foreign institutions, was late in taking preventive actions, and even snubbed scientists' offers of assistance".[27] This led to thousands of cases and hundreds of deaths.

In March 2020, Indonesia launched its contact tracing app, PeduliLindungi ("CareProtect"), which works in a similar way to Singapore's TraceTogether.[28] Available for iOS and Android devices, it alerts users of high-risk areas and when they may have been in close contact with persons infected with Covid-19.[29] However, the app has evolved to function as an immunity passport too; those who have been partially or fully vaccinated can use PeduliLindungi to access public transportation and other places requiring vaccination status, including supermarkets where use of the app became mandatory in September 2021.[30] However, in the same month, the government also announced that those without the app could still travel by plane or train as their Covid-19 health status could be checked though their personal identification number (NIK) when buying tickets.[31]

Israel

In addition to numerous lockdowns and other measures imposed to combat Covid-19, Israel also saw the introduction of a range of technology-based interventions. For instance, in March 2020, then Prime Minister Benjamin Netanyahu proposed the use of cyber surveillance techniques, originally designed to fight terrorism, to monitor people who have been in contact with those infected with Covid-19.[32] However, this real-time monitoring, carried out by Israel's

---

[25] Chile Today. (25 May 2021). *Chilean mobility pass promises more freedoms for the vaccinated.* Available at: https://chiletoday.cl/chilean-mobility-pass-promises-more-freedoms-for-the-vaccinated/

[26] Ciper Chile. (22 April 2020). *Problemas de protección de los datos personales de la aplicación "CoronApp".* Available at: https://www.ciperchile.cl/2020/04/22/problemas-de-proteccion-de-los-datos-personales-de-la-aplicacion-coronapp/

[27] KrASIA. (22 April 2020). *Indonesians skeptical of the state's COVID-19 prevention apps.* Available at: https://kr-asia.com/indonesians-skeptical-of-the-states-covid-19-prevention-apps

[28] Ibid.

[29] Pedulilindungi. (ND). *Pedulilindungi* (landing page). Available at: https://www.pedulilindungi.id

[30] Tempo. (7 September 2021*). PeduliLindungi App Mandatory in Supermarkets Starting Sept. 14.* Available at: https://en.tempo.co/read/1503232/pedulilindungi-app-mandatory-in-supermarkets-starting-sept-14

[31] Indonesia Expat. (27 September 2021). *PeduliLindungi: Trains and Planes Can be Booked Without App in October*. Available at: https://indonesiaexpat.id/news/pedulilindungi-trains-and-planes-can-be-booked-without-app-in-october/

[32] Aljazeera. (15 March 2020). *Israel to use 'anti-terror' technology to counter coronavirus.* Available at: https://www.aljazeera.com/news/2020/3/15/israel-to-use-anti-terror-technology-to-counter-coronavirus

domestic security service Shin Bet, was challenged in the Supreme Court,[33] andwas eventually struck down and banned by the Court.[34] Separately, the Health Ministry released HaMagen (*the Shield)* in March 2020. The country's first attempt at a contact tracing app, it was plagued by bugs and false positives.[35] The app was then revamped in July 2020.[36]

Israel was one of the first countries to release a Covid-19 passport when it announced the launch of the Traffic Light (Ramzor) app for iOS and Android devices in February 2021. This was also around the time that the government "approved the reopening of stores, gyms, hotels, and other venues".[37] Among other things, the app allows users to show their "Green Pass", a document containing a QR code showing that the user has either been vaccinated or recovered from Covid-19, which in turn permits access to a number of businesses and other spaces, such as restaurants, tourist attractions, museums, gyms, cultural events, places of worship, and a number of other places.[38]

Netherlands

When the Dutch government imposed the country's second national Covid-19 lockdown in January 2021 in response to the UK variant,[39] the Netherlands lagged behind other EU countries with its vaccine rollout. At that time, around 70,000 people had been given their first dose.[40] Included in the restrictions was a curfew between 20:30 and 4:30 during which people had to stay indoors and were only permitted to go out in limited circumstances. Such measures sparked violent protests[41] as well as legal proceedings challenging their constitutionality.[42] These measures were eventually lifted in the summer, but the government reintroduced restrictions in July after admitting that the "infection rate in the Netherlands has increased much faster than expected since society reopened almost completely".[43] New positive cases at that time had risen from a rolling seven-day average of 49 per million people to around 330 within a few days in July.[44]

---

[33] Reuters. (19 March 2020). *Israel orders citizens to stay home in partial lockdown.* Available at: https://www.reuters.com/article/us-health-coronavirus-israel-idUSKBN21622D

[34] Reuters. (1 March 2021). *Israeli Supreme Court bans unlimited COVID-19 phone tracking.* Available at: https://www.reuters.com/article/us-health-coronavirus-israel-surveillanc-idUSKCN2AT279

[35] The Times of Israel. (27 April 2020). *I wasted 2 days holed up in my bedroom thanks to buggy Health Ministry virus app.* Available at: https://www.timesofisrael.com/i-wasted-2-days-holed-up-in-my-bedroom-thanks-to-buggy-health-ministry-virus-app/

[36] The Times of Israel. (27 July 2020). *Health Ministry launches revamped COVID-19 tracking app.*Available at: https://www.timesofisrael.com/health-ministry-launches-revamped-covid-19-tracking-app/

[37] The Times of Israel. (18 February 2021). *Government launches Green Pass for vaccinated, warns fraudsters will be jailed.* Available at: https://www.timesofisrael.com/government-launches-green-pass-for-vaccinated-warns-of-jail-for-fraudsters/

[38] Ibid.

[39] Government of the Netherlands. (20 Januari 2021). *Lockdown measures tightened in response to concerns about new variants of virus.* Available at: https://www.government.nl/latest/news/2021/01/20/lockdown-measures-tightened-in-response-to-concerns-about-new-variants-of-virus

[40] BBC News. (16 February 2021). *Covid: Dutch crisis as court orders end to Covid curfew.* Available at: https://www.bbc.co.uk/news/world-europe-56084466

[41] Ibid.

[42] Verfassungsblog. (22 April 2021). *COVID-19 in the Netherlands: of Changing Tides and Constitutional Constants.* Available at: https://verfassungsblog.de/covid-19-in-the-netherlands-of-changing-tides-and-constitutional-constants/

[43] Government of the Netherlands. (9 July 2021). *No choice but to take summertime measures in face of rapid increase in infections.* Available at: https://www.government.nl/latest/news/2021/07/09/no-choice-but-to-take-summertime-measures-in-face-of-rapid-increase-in-infections

[44] The Guardian. (12 July 2021). *Dutch PM sorry for early reopenings as France tightens Covid rules.* Available at: https://www.theguardian.com/world/2021/jul/12/eu-nations-reimpose-covid-measures-as-cases-surge

The above timeline provides important context to CoronaCheck, the Netherlands' official immunity passport; vaccines were viewed by the government as the key to reopening the economy.[45] As such, the app was updated in June to allow users to display either a negative Covid test, vaccination or proof of recovery to access public venues requiring such information.[46] The information is contained in a QR code that venue organizers can scan using the Scanner Voor CoronaCheck app. In July 2021, the Dutch government announced that CoronaCheck could also be used to travel to EU countries using the EU's Digital Covid Certificate.[47] The app is available for iOS and Android devices and was initially made mandatory for entry into certain venues requiring a Covid pass (including festivals, dance venues and other events)[48] and for those travelling to the Netherlands.[49]

Tunisia

Despite the Arab Spring in 2011, which saw uprisings against tyrannical states across the Middle East, Tunisia remains a fragile democracy. Many citizens have grown frustrated with the continuing economic turmoil and political corruption, all of which have been exacerbated by the Covid-19 pandemic.[50] In addition to the tourism industry being decimated, the virus caused hospitals to be overwhelmed with infected patients.[51] During this crisis, the President of Tunisia, Kais Saied, usurped more powers, seemingly justified by the emergency caused by Covid-19; Parliament was suspended and the Prime Minister fired.[52]

Numerous presidential decrees were enacted to introduce measures to deal with Covid-19. These include a range of technology-based measures, a key one of which is E7mi, Tunisia's digital Covid-19 contact tracing app. It identifies and alerts users who may have had contact with others infected with the virus. According to the Tunisian government, the app is designed to save state resources and speed up the detection and treatment of infected patients. The app was released in May 2020 and is available for iOS and Android devices. While use of E7mi is not mandatory for residents of Tunisia, foreign visitors are required to download the app before entering the country.[53]

Western Australia

Even after Australia decreed nationwide measures against Covid-19, individual state authorities, including Western Australia, continued to implement their own measures to stop the spread of the virus. These included banning domestic travel and closing Western Australian borders in

---

[45] The Guardian. (3 May 2021). *Covid vaccine rollout rapidly gathering pace across Europe.* Available at: https://www.theguardian.com/world/2021/may/03/covid-vaccine-rollout-rapidly-gathering-pace-across-europe

[46] Government of the Netherlands. (18 June 2021). *Netherlands to take big step in relaxing measures: almost everything allowed with 1.5-metre distancing.* Available at: https://www.government.nl/latest/news/2021/06/18/netherlands-to-take-big-step-in-relaxing-measures-almost-everything-allowed-with-1-5-metre-distancing

[47] https://www.government.nl/topics/coronavirus-covid-19/news/2021/07/26/the-netherlands-adjusts-policy-on-travelling-within-eu

[48] https://www.government.nl/latest/news/2021/06/18/netherlands-to-take-big-step-in-relaxing-measures-almost-everything-allowed-with-1-5-metre-distancing

[49] https://www.government.nl/latest/news/2021/07/26/the-netherlands-adjusts-policy-on-travelling-within-eu

[50] https://open.spotify.com/episode/5FG6Zd4tBaJKCmCkwj7N4Y?go=1&sp_cid=cdb4d16ae91848d98d2a30102872af5c&t=1558&utm_source=embed_player_p&utm_medium=desktop&nd=1

[51] https://www.reuters.com/business/healthcare-pharmaceuticals/tunisia-says-health-care-system-collapsing-due-COVID-19-2021-07-08/

[52] https://open.spotify.com/episode/5FG6Zd4tBaJKCmCkwj7N4Y?go=1&sp_cid=cdb4d16ae91848d98d2a30102872af5c&t=1558&utm_source=embed_player_p&utm_medium=desktop&nd=1

[53] https://www.visatunisia.com/travel-restrictions-for-tourist/

April 2020.[54] Some measures were also technology-based, with the local government announcing in August 2020 GPS tracing bracelets and increased surveillance for high-risk hotel quarantiners following a handful of escapes[55]

Another example of these technological measures is SafeWA, the official contact tracing app for Western Australia launched in November 2020. At the time of its release, registering their attendance using QR codes with the app was mandatory for those wanting to access certain venues and events.[56] This included restaurants, bars, nightclubs, places of worship, beauty salons, cinemas, zoos, hotels, gyms, and libraries.[57] The information collected by venue and event organizers is then passed on to WA Health to use for contact tracing purposes. SafeWA can be used on iOS and Android devices.

Global Apps

The concept of an immunity passport predates the Covid-19 pandemic as far back as the 1880s during outbreaks of smallpox when public schools required students and teachers to show vaccination cards.[58] Proof of vaccination against yellow fever is also required today to enter countries such as Australia and India.[59] Even the digitization of these certificates is not new, as the Nigerian government proposed in 2019.[60]

As such, immunity passports have long been a mechanism to allow travel to continue even during a pandemic. Thus, as Covid-19 vaccines started being produced and distributed around the world, the travel sector pushed for the introduction of a passport to revive their industry by permitting people to travel based on their vaccination status. Two apps that have emanated from this push and are included in the scope of our report are CommonPass and IATA Travel Pass.

CommonPass

The CommonPass app was launched by the Commons Project Foundation (supported by the Rockefeller Foundation) and the World Economic Forum as a "digital health pass for travellers to securely document their certified Covid-19 test status while keeping their health data private".[61] It is built on the CommonPass Framework that "establishes standard methods for lab results and vaccination records to be certified and enables governments to set and verify their own health criteria for travellers".[62] Users of the app can share either their proof of vaccination or a negative Covid-19 test to be permitted to travel to different countries. It works with participating vaccine administrators or testing laboratories that provide SMART Health Cards and the app provides a user's health information via a QR code that can be scanned. Trials for the app began in October 2020 with Cathay Pacific Airlines and United Airlines taking part for

[54] https://www.watoday.com.au/national/western-australia/a-timeline-of-wa-s-covid-19-response-was-our-success-luck-good-management-or-a-bit-of-both-20200827-p55q03.html
[55] https://www.abc.net.au/news/2020-08-20/ankle-bracelets-may-be-used-to-enforce-hotel-quarantine-in-wa/12577496
[56] https://safewa.health.wa.gov.au
[57] https://www.watoday.com.au/national/western-australia/cafe-bar-check-ins-to-be-mandatory-in-wa-from-december-5-20201125-p56hx6.html
[58] https://www.nytimes.com/2020/12/13/technology/coronavirus-vaccine-apps.html
[59] https://practio.co.uk/travel-health/articles/vaccination-certificate
[60] https://www.bh4a.com.ng/2019/06/28/fg-phases-out-old-yellow-card-replaces-with-new-electronic-version/.
[61] CommonPass Digital Health Pass and Global Trust Framework Launches to Enable Safer Travel and Accelerate Border Reopenings: https://static1.squarespace.com/static/5ed685211872ca0609188980/t/5f7e26d37881542e8577278b/1602102995911/commonpass-pilot-pr-final-0.6.2020.pdf
[62] Ibid.

flights between London, New York, Hong Kong and Singapore.[63] The app is available for iOS and Android devices.

IATA Travel Pass

IATA Travel Pass is an app launched by the International Air Transport Association (IATA) and Evernym, a US company that develops verifiable credential technology. It allows travellers to "store and manage their verified certifications for Covid-19 tests or Covid-19 vaccinations".[64] The app forms part of the IATA Travel Pass Initiative, which comprises four modules that allow users to collate the health information required to meet the requirements of the travel destination.[65] The information is contained in a digital passport on the app that can be shared with airlines and authorities to facilitate travel.[66] IATA Travel Pass can also be used to digitally manage travel documentation throughout the journey.[67] It can be downloaded for iOS and Android devices.

[63] Ibid.
[64] IATA Travel Pass Q&A: https://www.iata.org/contentassets/2b02a4f452384b1fbae0a4c40e8a5d0c/travel-pass-faqs.pdf
[65] Ibid.
[66] Ibid.
[67] Ibid.

Covid Apps Comparison Table					
Country or Region	**App Name**	**Developer(s)**	**Launch Date**	**Functionality**	**Mandatory**
Australia	COVIDSafe	Australian Department of Health	April 2020	Contact Tracing	No
Bahrain	BeAware Bahrain	Information & eGovernment Authority Bahrain	February 2021	Contact Tracing and Immunity Passport	No
Chile	CoronApp	Gobierno Digital	April 2020	Self-Diagnosis and Information Dissemination	No
Indonesia	PeduliLindungi	The Ministry of Communication and Information of the Republic of Indonesia	March 2020	Contact Tracing and Immunity Passport	Yes
Israel	Ramzor	Israel's Ministry of Health	February 2021	Immunity Passport	Yes
Netherlands	CoronaCheck	Rijksoverheid	June 2021	Immunity Passport	Yes (for selected venues)
Netherlands	Scanner Voor CoronaCheck	Rijksoverheid	June 2021	Immunity Passport	Yes (for selected venues)
Tunisia	E7mi	Tunisia's Observatory of Emerging Diseases (ONME) and Wizzlabs (IT services start-up headquartered in Tunis)	May 2020	Contact Tracing	Yes (for foreigners)
Western Australia	SafeWA	Department of Health of the Government of Western Australia	November 2020	Contact Tracing	Yes
Global	CommonPass	The Commons Project Foundation and the World Economic Forum	October 2020	Immunity Passport	No
Global	IATA Travel Pass	International Air Transport	April 2021	Immunity Passport	No

		Association and Evernym			

Covid-19: Policy, Legal & Technical Trends and Recommendations

Pillar 1 - Public Health Efficacy

Engagement with evidence-based policymaking

To respond to any emergency, it is imperative that governments engage in evidence-based policymaking. This means that policies and measures attempting to address the emergency should have a sound underlying rationale to ensure that they are effective. Thus, in the context of the Covid-19 pandemic, any public health interventions should be tailored to the specific conditions of the country or region and supported by relevant scientific research.

Were countries adequately prepared for the rollout of Covid apps to ensure their effectiveness in combatting the virus?

Launching a mobile application as a prominent part of the response to a public health emergency is unprecedented. Covid apps, namely contact tracing apps and immunity passport apps, were rolled out in many countries. Both were viewed as an opportunity to take advantage of modern technology to suppress Covid-19 effectively and efficiently.

However, to take full advantage of the potential benefits of these apps, governments must prepare the ground to ensure the success of these technological interventions: certain infrastructure needs to be in place to ensure that the use of Covid apps is feasible for a sufficient proportion of the population.

Of particular importance in this regard is critical internet infrastructure. Research has shown that, during the pandemic, there was a significant increase in internet bandwidth consumption globally, fuelled by a rise in consumer adoption of mobile apps.[68] It is therefore crucial that access to the internet is adequately distributed across the population to ensure that those downloading Covid apps can make use of them.

The table below shows some of the important elements of critical internet infrastructure across the countries covered in our report.

[68] https://sensortower.com/blog/app-download-data-usage-growth

Internet and Mobile Technology Infrastructure in Countries of Focus					
Country	Population[69]	Urban Population	Secure Internet Servers (per 1m people, 2020)[70]	Mobile Cellular Subscriptions (per 100 people, 2020)[71]	Internet Usage (% of population)[72]
Australia	25,499,884	86%	39,804	108	86.55%
Bahrain	1,701,575	89%	392	103	99.54%
Chile	19,116,201	85%	12,814	131	82.33%
Indonesia	273,523,615	56%	513,564	130	53.73%
Israel	8,655,535	93%	12,349	132	86.9%
Netherlands	17,134,872	92%	136,866	125	93.29%
Tunisia	11,818,619	70%	328	126	66.7%

This table shows statistics for secure internet servers, mobile cellular subscriptions and internet usage in the seven countries of focus. Also included is the total population of each country and the percentage of those living in urban areas (i.e., areas that tend to be more developed with better infrastructure relative to rural areas). Theoretically, the more internet servers available, the more mobile cellular subscriptions can be obtained, therefore resulting in higher access to and use of the internet. However, it can be assumed that better internet infrastructure will most likely be found in urban rather than rural areas of a country. Accordingly, internet usage may predominantly derive from urban areas, thus potentially exposing a digital divide between urban and rural populations within a particular country. This is in addition to the digital divide evident between countries: in the developed world, internet access is around 87% on average, compared to 47% in developing countries and only 19% in the least developed countries.[73]

This is an important point since the level of internet access can have an impact on the uptake of Covid apps, which in turn can determine their efficacy from a public health perspective. This was shown in a study in the University of Oxford from April 2020, which found that while uptake levels for contact tracing apps as low as 14% can help reduce the spread of Covid-19, a 56% uptake would be needed to suppress Covid-19 completely.[74] However, a more recent study using data from the Copenhagen Network Study in March 2021 showed that uptake levels of 20% could lead "to a decrease in daily new cases even with the least restrictive policy".[75] The higher the number of people that use contact tracing apps, the more effective public authorities can be at tracking the spread of Covid-19 and either: (i) warn individuals of

[69] Population stats from: https://www.worldometers.info/world-population/population-by-country/
[70] https://data.worldbank.org/indicator/IT.NET.SECR.P6?end=2020&locations=TN-BH-ID-CL-AU-NL-IL&most_recent_value_desc=true&start=2010&type=shaded&view=chart. The number of distinct, publicly trusted TLS/SSL certificates found in the Netcraft Secure Server Survey.
[71] https://data.worldbank.org/indicator/IT.CEL.SETS.P2?locations=TN-BH-ID-CL-AU-NL-IL. These are subscriptions to a public mobile telephone service that provide access to the Public Switched Telephone Network (PSTN) using cellular technology, including 3G and 4G subscriptions.
[72] https://data.worldbank.org/indicator/IT.NET.USER.ZS?locations=TN-BH-ID-CL-AU-NL This includes usage from a computer, mobile phone, personal digital assistant, games machine, digital TV etc.
[73] https://www.itu.int/en/ITU-D/Statistics/Documents/facts/FactsFigures2019.pdf (p.2)
[74] 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
[75] https://www.nature.com/articles/d43978-021-00034-5

potential infection if they have been in close contact with infected persons; (ii) warn people generally of potential infection hotspots; or (iii) make more informed decisions about where to impose lockdowns or other restrictive measures to stop the spread of the virus.

The table below sets out the different uptake levels for the contact tracing apps covered in our report.

Uptake of Contact Tracing Apps		
App	Country/Region	Uptake (% of population)[76]
COVIDSafe	Australia	28.4%
BeAware Bahrain	Bahrain	25%
PeduliLindungi	Indonesia	18.3%
SafeWA[77]	Western Australia	17.8%
E7mi	Tunisia	0.8%

As shown above, Australia's COVIDSafe had the highest uptake at 28.4%. Thus, at least in theory, the app had a high enough uptake level to help stem the spread of Covid-19. In terms of internet infrastructure, the country has over 39,000 secure internet servers per million people, enabling 108 mobile cellular subscriptions per 100 people. This results in an internet usage of 86.55%, with 86% of people living in urban areas likely to have better-developed internet infrastructure and therefore where internet usage may be most concentrated. Furthermore, Australia has a relatively minimal digital divide, meaning that there may be a better distribution of internet access across the country, thus avoiding the risk that app use is only feasible in limited places.

By comparison, Indonesia's contact tracing app, PeduliLindungi, achieved a lower uptake of 18.3%. In this country, there are over 500,000 secure internet servers per million people and 130 mobile cellular subscriptions per 100 people. Despite this, internet usage is only 53.73% and only 56% of people live in urban areas where better-developed internet infrastructure is more likely. The digital divide is therefore quite severe in Indonesia, impacting the potential efficacy of PeduliLindungi since it may be difficult to access in rural areas of the country. A 2019 report by the World Bank found that 62% of adults were connected to the internet in urban areas, compared to 36% in rural areas. Accordingly, one of the policy recommendations made in that report is to "boost digital connectivity and universalize access to high quality internet".[78]

At 0.8%, Tunisia's E7mi is the contact tracing app with the lowest uptake among our countries of focus. The country has only 328 secure internet servers per million people and 126 mobile cellular subscriptions per 100 people. This enables an internet usage of 66.7%, which is higher than the average for Africa at 28.2% (the lowest of all the regions of the world).[79] Tunisia thus has relatively few internet servers that are likely located in urban areas where 70% of the total population lives, therefore exposing a digital

[76] Population stats from: https://www.worldometers.info/world-population/population-by-country/. Download numbers taken from stats available from Google Playstore.
[77] Population stats from: https://www.population.net.au/population-of-western-australia/. Download stats from Google Playstore: https://play.google.com/store/apps/details?id=au.gov.wa.health.SafeWA.
[78] https://www.worldbank.org/en/news/press-release/2021/07/28/ensuring-a-more-inclusive-future-for-indonesia-through-digital-technologies
[79] https://www.itu.int/en/ITU-D/Statistics/Documents/facts/FactsFigures2019.pdf (p.2)

divide that is evident across the continent as a whole. The World Bank has found that "there are growing digital divides in [mobile internet] use between richer, urban, literate, and better educated households with electricity and poorer households without electricity".[80] This may explain the especially poor uptake of E7mi in Tunisia.

Of course, achieving a sufficient uptake level for contact tracing apps not only requires an adequate distribution of internet access across the population. Income levels, for instance, can significantly influence whether people can afford mobile cellular subscriptions or even mobile phones. In addition, even if the app has been downloaded, it may not always be used as intended; in Western Australia, for instance, the number of check-ins recorded on SafeWA by users began to fall a few weeks after the app launched, raising fears from experts that low usage could make tracing a Delta outbreak more difficult.[81]

Nevertheless, internet infrastructure can still play a crucial role in the efficacy of digital contact tracing and other Covid apps. Thus, governments should take this into account for future responses to public health crises or other emergencies that may involve the launch of a mobile app or other web-based policies.

Does the scientific evidence sufficiently support the use of immunity passport apps?
As already mentioned, the rationale of immunity passport apps is that they enable people to demonstrate that there is a low risk of them spreading Covid-19 to others, thereby allowing them to enter public venues and interact with others. It can sometimes also mean that other restrictions or measures, such as social distancing or mask mandates, do not need to be applied to those with valid immunity passports.

Typically, there are three pieces of health information that immunity passport apps are designed to store and display when required: vaccination status, the results of a recent Covid test, or evidence of natural immunity developed after recovering from Covid-19. Thus, the presumption is that one or a combination of these pieces of information prove that a person is not infected with the virus and/or is unlikely to pass the virus on to another person. With that being the case, it is therefore important that the health information displayed by immunity passport apps is sufficient to demonstrate the mitigation of the risk of spreading Covid-19. This in turn would support the argument that such an app would be fit for purpose, which in turn would underpin arguments for the necessity and proportionality of such a measure.

To determine whether that health information is sufficient for the risk mitigation task, governments ought to confirm whether the scientific evidence suggests that such information can demonstrate the mitigation of the risk. For example, with Covid-19 vaccines, the nature of the protection provided by such vaccines should be established before requiring people to show their vaccine status to gain entry to public venues. In other words, scientific research should be conducted to identify whether the vaccine (a) prevents a person from contracting Covid-19 and (b) prevents a person who has contracted Covid-19 from passing it on to another person. These questions have been raised throughout the pandemic, including during the outbreak of the Omicron variant.[82]

[80] https://www.worldbank.org/en/news/feature/2021/09/24/narrowing-the-digital-divide-can-foster-inclusion-and-increase-jobs
[81] https://www.abc.net.au/news/2021-10-09/experts-concerned-by-low-safe-wa-usage-rates/100521922
[82] https://www.reuters.com/business/healthcare-pharmaceuticals/moderna-ceo-says-vaccines-likely-less-effective-against-omicron-ft-2021-11-30/; https://www.nature.com/articles/d41586-021-03614-z

In December 2020, Pfizer released its study showing that, after two doses, its vaccine is 95% effective in preventing Covid-19.[83] Around the same time, Moderna reported vaccine effectiveness of 94.5% after two doses.[84] In February 2021, AstraZeneca found that its vaccine was 82% effective after two doses.[85] However, whilst vaccines can reduce virus transmission, they cannot fully prevent it.[86] Furthermore, the protection provided by vaccines has been shown to decrease over time, especially as other variants emerge.[87] Thus, later studies have found that vaccine efficacy "is lower for Omicron than for other variants and tends to wane over time".[88]

This shows that a person's vaccine status alone may not always be sufficient to show that they are at a lower risk of spreading Covid-19. It is therefore important that immunity passport apps give users the ability to show other health information that would – taken together – better demonstrate a lower risk of spreading the virus.

The table below shows the immunity passport apps covered in our report and the health information that can be displayed by them.

Health Information in Immunity Passport Apps				
App	**Country/Region**	**Vaccine Status**	**Covid Test Result**	**Natural Immunity**
BeAware Bahrain	Bahrain			
PeduliLindungi	Indonesia			
Ramzor	Israel			
CoronaCheck	Netherlands			
CommonPass	Global			
IATA Travel Pass	Global			

Green = Yes, Red = No

As shown above, the Netherlands and Israel represent what is perhaps best practice by designing their respective apps to display a full range of relevant health information to demonstrate a person's risk of spreading Covid-19. By contrast, Indonesia's immunity passport app only allows users to show their vaccine status but not a negative Covid test or evidence of natural immunity. Neither CommonPass nor IATA Travel Pass allow users to show evidence of natural immunity.

Were the relevant public health authorities adequately involved in the public health response?

Public health emergencies require public health expertise. Accordingly, for the Covid-19 pandemic, it is critical that governments work with the relevant public authorities to assemble pertinent advice that helps formulate the most effective policies and measures to respond to the emergency. This means implementin structures that ensure that public health authorities are

[83] https://www.nejm.org/doi/full/10.1056/NEJMoa2034577?query=RP
[84] https://www.fda.gov/media/144434/download (p.5)
[85] https://www.astrazeneca.com/media-centre/press-releases/2021/COVID-19-vaccine-astrazeneca-confirms-protection-against-severe-disease-hospitalisation-and-death-in-the-primary-analysis-of-phase-iii-trials.html
[86] https://www.thelancet.com/journals/laninf/article/PIIS1473-3099(21)00648-4/fulltext; https://www.imperial.ac.uk/news/231557/covid-vaccines-effective-household-transmission-delta/
[87] https://www.nature.com/articles/d41586-021-02532-4
[88] https://www.ema.europa.eu/en/news/preliminary-data-indicate-COVID-19-vaccines-remain-effective-against-severe-disease-hospitalisation

involved in the decision-making process and that the relevant advice is supplied in a consistent and effective manner.

Implementing this can be particularly challenging in countries that have federalized political systems where local authorities can make public health decisions independently of national authorities. In Australia, the Australian Health Protection Principal Committee (AHPP) was created in 2009 to "provide advice and recommendations to the Australian Health Ministerial Advisory Council and National Cabinet".[89] The National Cabinet comprises the Australian Prime Minister and State and territory premiers and chief ministers.[90] For the Covid-19 pandemic, the Australian government ensured that a structure was put in place to enable scientific advice to flow from experts to decision-makers to inform the public health response at both the local and national levels.[91] Australia is therefore an example of a country that took a decentralized approach to its Covid-19 strategy. Individual states were able to enact their own measures for Covid-19, including technological interventions such as the SafeWA contact tracing app in Western Australia, to achieve a more tailored approach for local populations.[92]

However, other governments chose to centralize health policy to deal with Covid-19. For example, the Tunisian government created a National Covid-19 Monitoring Authority, headed by the President, to monitor and evaluate the progress of Covid-related measures. Its mandate includes "monitoring the regularity of the supply of basic products, the distribution of social assistance to poor families or families without income, as well as the referral of recommendations to the national committee to combat Covid-19 to adopt the necessary measures to contain the virus".[93] Whilst this kind of centralization could enable greater efficiency and more consistent measures across the populace, it can be insensitive to the nuances present at the local level. This was the case in Tunisia where local authorities took issue with a circular sent out by the President requiring them not to enact measures that are inconsistent with the government's approach to Covid-19.[94]

Even where public authorities are involved in the decision-making process, it is also important that such authorities are subject to transparency and accountability. This can help bolster the quality and legitimacy of their work and the advice provided to policymakers. In the Netherlands, the Dutch National Institute of Public Health (RVIM) set up an Outbreak Management Team (OMT), which brings together different experts to "discuss how to control the outbreak based on the latest information, their own professional expertise and available scientific literature".[95] However, in addition to providing advice to the RVIM and the government, the reports produced by the OMT and the identity of the group's members are made public.[96] Moreover, the OMT has also had to defend its reports in the Dutch legislature.[97]

[89] https://www.directory.gov.au/portfolios/health/department-health/australian-health-protection-principal-committee
[90] https://www.pm.gov.au/media/advice-coronavirus
[91] https://theconversation.com/4-ways-australias-coronavirus-response-was-a-triumph-and-4-ways-it-fell-short-139845
[92] https://www.mckinsey.com/industries/public-and-social-sector/our-insights/collaboration-in-crisis-reflecting-on-australias-Covid-19-response
[93] https://www.oecd.org/coronavirus/policy-responses/Covid-19-crisis-response-in-mena-countries-4b366396/
[94] https://nawaat.org/2020/05/06/Covid-19-in-tunisia-tensions-arise-between-municipalities-and-central-government/
[95] https://www.rivm.nl/en/coronavirus-covid-19/omt
[96]
[97] https://blogs.lse.ac.uk/europpblog/2020/05/18/democracy-experts-should-seek-a-central-role-in-shaping-the-post-coronavirus-order/

Recommendation: *Governments should ensure that the relevant critical infrastructure is in place to ensure that technological measures introduced to address a public emergency are as effective as possible. Especially in the context of mobile apps or other web-based services, internet infrastructure should be developed so that internet access is sufficiently distributed across the population to support the network usage that such interventions may require.*

Recommendation: *Technological measures used in response to a public health emergency should have an underlying rationale based on relevant scientific research to ensure that such measures effectively address the emergency.*

Recommendation: *Public health authorities or other bodies comprising relevant experts should be adequately involved in the decision-making process so that policymakers can ensure and demonstrate that their interventions are based on relevant research and thus appropriate for the particular circumstances of the emergency being addressed.*

Lack of public awareness of the scientific research underpinning Covid measures

Covid-19 rapidly spread across the world and presented a novel type of risk for most people. The learning curve was therefore steep for governments and citizens alike, and – particularly early on – required action on the basis of limited knowledge. Many places also saw a surge in conspiracy theories surrounding the disease, including among political actors.
There is growing evidence that adherence to social distancing and quarantining, as well as vaccination incentives, are strongly influenced by well-designed public awareness campaigns. These campaigns can be considered to be well-designed if they take into account the plurality of people in any country; age, gender, ethnicity, whether someone is part of a marginalized group, and other factors can have a significant impact. Successful public awareness campaigns consider different media consumed by the target demographic (e.g., social media instead of television, or vice versa). In a number of places, these campaigns have contributed to more proactive adherence to public health measures, local production of facemasks where these were not available, and willingness to be vaccinated. The role of the government is not just to facilitate by creating central points where people can access information (or vaccinations), but to actively spread important information, both on- and offline, in neighborhoods and online communities.[98,99,100] These strategies must not just be top-down, but include public figures and especially trusted people in local communities, e.g., local social and medical workers, schools, religious organizations, charities and employers, different levels of government (state,

[98] https://www.mdpi.com/2227-9709/8/4/80
[99] https://www.weforum.org/projects/COVID-19-customised-and-targeted-awareness-campaign
[100] https://www.worldbank.org/en/news/feature/2020/06/28/awareness-campaigns-help-prevent-against-covid-19-in-afghanistan

provincial/state, local).[101] These "coalitions of the willing" can significantly enhance the efficacy of public health measures, save lives, potentially limit the need for more restrictive measures, and strengthen the ties between the government and civil society.

Recommendation: *Create "coalitions of the willing" with broad representation from civil society. Awareness campaigns, both on- and offline, can facilitate adherence to public health measures and prevent loss of trust. Take into account the different demographics, particularly of marginalized communities, and work with trusted groups within those communities.*

Efficacy of public procurement during Covid-19

In emergency situations, governments often rely on external organizations to acquire the necessary equipment, expertise or other resources to deal with the emergency and execute certain policies. In the context of Covid-19, many countries relied on such organizations, both domestic and international, to obtain medical equipment, PPE, ventilators, beds, Covid tests, and vaccines to combat the virus.

Typically, public procurement can be a lengthy and cumbersome process. Under most laws, the competitive process for negotiating contracts with suppliers can take months or even years, as is the case under the UNCITRAL Model Law on Public Procurement.[102] Furthermore, the process requires quite intense due diligence to take place to ensure the security of the acquisition; under the UNCITRAL Model Law, the procuring entity must evaluate the potential buyer against elaborate criteria, including the price and the terms of payment and guarantee in respect of the subject matter of the procurement.[103]

Clearly, such a process is not suitable for an emergency where time is of the essence. Some legal frameworks therefore make provision for an expedited version of the procurement process that allows governments to acquire the resources needed to respond to the emergency at hand quickly and effectively. For example, in the Netherlands, the Dutch Public Procurement Act permits a simplified procedure that is not subject to the usual timescale in cases of extreme urgency.[104]

However, where comprehensive expedited processes for public procurement are not in place or followed, this can create a range of problems that may reduce the effectiveness of the goods and services acquired by the state.[105] In Australia, for example, the government's botched Covid vaccine rollout last year was blamed on the poor performance of the private companies

[101] https://gtmr.org/wp-content/uploads/2021/06/June-2021-Recommendations-VTF-06112021.pdf
[102] Article 6 of the United Nations Commission on International Trade Law Model Law on Public Procurement, https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/en/2011-model-law-on-public-procurement-e.pdf.
[103] Article 11.1 of the United Nations Commission on International Trade Law Model Law on Public Procurement, https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/en/2011-model-law-on-public-procurement-e.pdf.
[104] https://www.twobirds.com/en/news/articles/2020/global/COVID-19-urgency-in-procurement-and-tenders
[105] Arrowsmith et al, 'Public Procurement Regulation in (a) Crisis? General Introduction', in Arrowsmith et al, *Public Procurement Regulation in (a) Crisis?* (Hart Publishing, 2021).

involved, with multiple reports of "vaccines not showing up on the scheduled delivery day...or of immunization workers not appearing on the scheduled delivery day".[106] Consequently, in August 2021, according to *The Financial Times*, only 15% of Australians were fully vaccinated, which at the time was one of the lowest rates in the developed world.[107] This illustrates how emergencies can make it more difficult to acquire the necessary resources from reliable suppliers. In Tunisia, the government sought to acquire 400,000 Covid-19 rapid test kits from China which seemingly never arrived.[108]

Given these examples of inefficacy in the context of public procurement, which can also be found in other countries, governments should ensure that alternative procedures are implemented which are appropriate for urgent procurement cases. Such procedures should allow contracts to be finalized swiftly and ensure that goods or services are delivered on time and on optimal terms (i.e., in relation to price and quality).[109] In addition, governments could also set up advance purchasing arrangements for possible emergencies that may help to "secure rapid and reliable delivery and better security of supply".[110]

Recommendation: *Have in place permanent, as opposed to ad hoc, rules for public procurement for emergencies to ensure increased efficacy of the acquisition of goods or services. This could also be coupled with advance purchasing arrangements to quickly secure goods and services that may be needed to address the emergency in question.*

[106] https://www.theguardian.com/society/2021/apr/11/australias-covid-vaccination-relying-on-opaque-private-contracts-worth-millions
[107] https://www.ft.com/content/3637a08d-f9cb-436e-9053-5563a29b1edd
[108] https://arij.net/investigations/tunisian-government-covid-19/
[109] Arrowsmith el al, 'The Approach to Emergency Procurement in the UNCITRAL Model Law: A Critical Appraisal in Light of the Covid-19 Pandemic', in Arrowsmith et al, *Public Procurement Regulation in (a) Crisis?* (Hart Publishing, 2021).
[110] Ibid.

Pillar 2 - Function Creep & Unintended Consequences

Function Creep

Lack of legal framework for Covid apps and other measures

In some of the countries of focus, the apps and measures deployed to combat Covid-19 were often unaccompanied by adequate legal frameworks to regulate their use. In particular, some governments failed to implement two important layers of regulation for Covid-related initiatives.

Were Covid apps underpinned by a sufficient legal basis?

The first layer consists of legislation that permits the state to create and deploy a Covid pass, whether in a digital or paper form (or both). This first legislative layer legally permits the existence of a Covid pass created and operated by the state. In Tunisia there is no legislation specifically permitting the deployment of the E7mi app or its Covid pass. Instead, the Tunisian government exercised broad and vague powers to deal with the repercussions of Covid-19. This was also the case in Western Australia; whilst part of the legal basis for SafeWA could be found in local legislation (the Protection of Information (Entry Registration Information Relating to Covid-19 and Other Infectious Diseases) Act 2021). It was passed seven months after the app was launched in November 2020.[111]

The second layer of legislation specifies the basis for the processing of the personal data required for the Covid apps to function. This essentially permits the processing of the personal data by the app, which may then be reflected in the corresponding privacy policy or notice. The processing of personal data carried out by the COVIDSafe app in Australia (which is for digital contact tracing) is regulated by new privacy legislation passed for Covid-related measures.[112] The law makes it an offence to use data collected by the app for any purpose other than contact tracing. Conversely, there is no explicit law regulating the use of personal data processed by Tunisia's contact tracing app (E7mi). In Indonesia, the data processing carried out by its contact tracing app, PeduliLindungi, is only regulated by two ministerial decrees against a backdrop of weak data protection laws. No specific agency is responsible for ensuring the enforcement of data protection rules.[113]

Without a legal basis for the existence of Covid apps or the processing of personal data, it is more difficult to identify and prevent function creep. If the law fails to specify when certain measures can be used or how they can be used (i.e., what data can be collected and what purpose(s) they can be used for), it makes it easier for the state to use these measures for initiatives beyond Covid-19. This could potentially lead to the abuse or undermining of individual rights. An example can be found in Australia, where both COVIDSafe (the national contact tracing app deployed by the federal government) and SafeWA (the contact tracing app for Western Australia) host personal data on servers provided by Amazon Web Services. The privacy policy for SafeWA states that local or foreign laws may require the disclosure of personal data by Amazon to government authorities in some limited circumstances.[114] This has

[111] https://www.legislation.wa.gov.au/legislation/prod/filestore.nsf/FileURL/mrdoc_43928.pdf/$FILE/Protection%20of%20Information%20(Entry%20Registration%20Information%20Relating%20to%20COVID-19%20and%20Other%20Infectious%20Diseases)%20Act%202021%20-%20%5B00-a0-00%5D.pdf?OpenElement

[112] https://www.legislation.gov.au/Details/C2020A00044

[113] https://kr-asia.com/indonesians-skeptical-of-the-states-covid-19-prevention-apps

[114] https://safewa.health.wa.gov.au/privacy

raised concerns about personal data collected via SafeWA being used for extraneous purposes. These fears were realised in June 2021 when it was found that the police had requested SafeWA data as part of criminal investigations, which was granted by the health authority in a number of these cases.[115] The Government of Western Australia became aware of this a month prior, in April 2021.[116] This then led the government to pass the Protection of Information (Entry Registration Information Relating to Covid-19 and Other Infectious Diseases) Act 2021 to prevent the police from using personal data from SafeWA;[117] this law prevents personal data collected by the app being used for purposes other than those related to contact tracing.

Another stark example of function creep observed in our countries of focus can be found in Bahrain. BeAware Bahrain, the country's digital contact tracing and immunity passport app, was used as part of a TV show called *Are You At Home?* — phone numbers gathered through the app were called live on air to check if users were staying home during Ramadan.[118] Participation in this TV program was initially mandatory for users until the government updated the app to allow users to opt out of the competition. However, the privacy policy for the app does not mention the use of personal data for participation in a live TV show. This would appear to be in contradiction of Bahrain's data protection laws, which state that information about the purposes for which data is intended to be processed should be provided to users.[119]

Did governments make provision in their legal framework for declaring a "state of emergency" to deal with the Covid-19 pandemic?

Preventing function creep that may result from insufficient legal frameworks does not always require ad hoc legislation to be passed during an emergency. States can make provision in their constitution or legal framework for a system for dealing with national emergencies, like a pandemic, allowing for limited derogations from the usual democratic processes to deal quickly with the emergency at hand. The Dutch constitution, for instance, allows the government to declare either a limited state of emergency or a general state of emergency "in order to maintain external or internal security".[120] This in turn gives the government the power to enact emergency provisions in existing laws or introduce special emergency laws stipulated in the Coordination Act for Exceptional Circumstances.[121] This may involve the restriction of human rights and fundamental freedoms. However, the legislature is empowered to decide on the duration of the state of emergency and still plays a key oversight role.[122]

These "states of emergency" can thus help to ensure continued oversight of the government while it implements measures to deal with the national emergency, in turn safeguarding human rights and the important functions of the different organs of the state. This is preferable to states exercising executive (or emergency) powers in an arbitrary manner with few limitations

[115] https://audit.wa.gov.au/wp-content/uploads/2021/07/Report_2__SafeWA-Application-Audit.pdf (p.7)
[116] https://theconversation.com/police-debacle-leaves-the-mcgowan-government-battling-to-rebuild-public-trust-in-the-safewa-app-162850
[117] https://www.abc.net.au/news/2021-06-16/police-refused-to-stop-accessing-safewa-app-data-premier-says/100218764
[118] https://www.amnesty.org/en/latest/news/2020/06/bahrain-kuwait-norway-contact-tracing-apps-danger-for-privacy/
[119] See Article 17(1)(b) of Law No. (30) of 2018 with Respect to Personal Data Protection Law, https://bahrainbusinesslaws.com/laws/Personal-Data-Protection-Law.
[120] Article 103, https://www.constituteproject.org/constitution/Netherlands_2008.pdf?lang=en
[121] https://wetten.overheid.nl/BWBR0007981/2018-01-01
[122] https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651972/EPRS_BRI(2020)651972_EN.pdf. However, it should be noted that a state of emergency has never been declared in the Netherlands during the Covid-19 pandemic. See https://verfassungsblog.de/covid-19-in-the-netherlands-of-changing-tides-and-constitutional-constants/

on their nature or scope, which arises due to other state organs being relegated to limited roles during the emergency itself. This can create the potential for abuse of power and function creep, which the state may argue is justified on the basis of an "emergency situation". An example of this can be found in Tunisia, where Covid-related measures were introduced in the midst of political turmoil that saw the executive usurp powers, the suspension of Parliament and the firing of the Prime Minister.[123] This allowed the President to implement measures arbitrarily through decrees without explicit limits on those interventions.

Regardless of whether legislation is passed during an emergency or defined prior to the state of emergency, having a sufficient legal framework during a national emergency like a pandemic is important not only to prevent function creep at the time of the emergency but also afterwards. This is because there can be a risk of measures introduced during an emergency becoming the new normal. More specifically, without the appropriate limitations imposed by law, there is the potential for technology-based measures, such as Covid apps, to crystalize into permanent parts of the surveillance apparatus of a state. For instance, in Indonesia, the privacy policy for the CareProtect app (which is used for contact tracing and to display an immunity passport) states that user data collected by the app will be deleted after the Government of Indonesia has declared the Covid-19 pandemic to be over.[124] However, no criteria have been set out as to how this decision is to be made or on what basis. Nor is it clear how this decision will be communicated to the public once it has been made or how the deletion of the data will be verified. In Bahrain, the BewareBahrain app was introduced in the context of the government's wider digital transformation agenda involving greater use of cloud technology, AI, blockchain and other initiatives.[125] Thus, Covid apps could easily be tacitly subsumed into these wider plans and adjusted to fit other contexts even when such contexts may not justify these technological interventions.

All this emphasizes the overall importance of having a sufficient regulatory framework to limit the nature and scope of these technological interventions to prevent their unjustified permanency.

> **Recommendation:** *Implement a comprehensive legal framework that provides a basis for the development of measures forming part of an emergency response. Most preferably, provision could be made in the country's constitution or legal system that enables the invocation of a "state of emergency" which, for a limited time, establishes modified roles for the different organs of the state during the emergency while also maintaining sufficient oversight and safeguards to protect individual rights.*

Privacy by design in Covid apps

Privacy by design is about integrating privacy principles into the design, development and deployment of systems that process personal data. This is especially important in relation to the systems and apps developed for combatting Covid-19, since this involves the collection and processing of sensitive data, such as medical information. Therefore, if these systems and apps

[123] https://open.spotify.com/episode/5FG6Zd4tBaJKCmCkwj7N4Y?go=1&sp_cid=cdb4d16ae91848d98d2a30102872af5c&t=1558&utm_source=embed_player_p&utm_medium=desktop&nd=1

[124] https://www.pedulilindungi.id/kebijakan-privasi-data

[125] https://english.alarabiya.net/views/news/middle-east/2020/08/13/Bahrain-s-BeAware-coronavirus-app-has-saved-lives-Here-s-how

are designed, developed and deployed with privacy built in, then sensitive data can be processed in a responsible and ethical manner while still fulfilling public health objectives.

However, the Covid apps covered in our report had varying levels of success in terms of achieving privacy by design. Where the implementation of the concept is poor, this can result in more severe privacy harms being suffered by users. Such harms can often take the form of app developers, as well as the governments soliciting their services, failing to properly uphold the privacy and data protection rights of individuals.

Was the personal data collected via Covid apps processed for specific purposes and limited to what was necessary?

One of the principles of privacy by design is that privacy should be the default setting. This means delivering "the maximum degree of privacy by ensuring that personal data are automatically protected in any given IT system or business practice".[126] In addition, no action should be "required on the part of the [user] to protect their privacy".[127] Two specific concepts can be used to implement this principle. The first is that personal data should be processed for specific and legitimate purposes (purpose limitation).[128] The second is that the personal data processed, in terms of both its volume and nature, should be limited to what is necessary to achieve the processing purpose (data minimization).[129]

In relation to the apps covered in this report, ensuring privacy as the default setting is particularly important when using software developer kits (SDKs) for building mobile apps. SDKs are software tools from third parties that developers can integrate into their own apps to help speed up the development process. There is a range of SDKs available that provide different features, including bug reporting, cryptographic support, analytics and advertising. However, the use of SDKs can pose privacy risks for the end-user, "especially when developers integrate proprietary SDKs offered by data-driven organisations like analytics and advertising companies".[130] Furthermore, current mobile operating systems use a permission-based model for apps, meaning that SDKs embedded in apps can access permission-protected resources such as location data.[131] Such data may thus become accessible to the developer or third parties and used for other unrelated purposes.

An example of potentially bad practice with respect to SDKs is the CommonPass app. Two notable software libraries used by this app are *Bugsnag* and *NewRelic*. Both apps monitor the performance of the app running on mobile devices and provide reports on app stability. The information included in such reports include network connectivity, Bluetooth status, battery levels and recording when the screen is turned on or off. Such data may be necessary for the purpose of service improvement, but the use of two SDKs for this purpose might mean that an excessive amount of data may be collected.

Another example is PeduliLindungi in Indonesia. A previous version of the privacy policy for the app admitted to the use of a third-party SDK that shared data with the third-party developer of the SDK.[132] Indeed, one of the permissions made by the app when running on a user's phone is access to location data to track the user's movements and notify them when they enter

[126] https://www.ipc.on.ca/wp-content/uploads/resources/7foundationalprinciples.pdf
[127] Ibid.
[128] https://iapp.org/resources/article/fair-information-practices/
[129] Ibid.
[130] *Data Protection and Privacy: Data Protection and Artificial Intelligence*, Hart Publishing, 2021 (p.2).
[131] Tech Report, p.25.
[132] See p.51 of the Tech Report.

a certain geographical area. As PeduliLindungi is a contact tracing app, location data is used to alert users to areas with high Covid-19 infection rates or when they may be in close contact with a person infected with the virus. However, sharing this information with the developer of the SDK appears to be unnecessary and the policy itself did not specify the reason for this data sharing.

In Western Australia, the SafeWA contact tracing app uses the *Google Firebase* and *Sentry* SDKs. Both third-party components can be used for tracking a range of activities within the app and make automatic reports on these activities. It has been observed that such tracking information is recorded by one or both of these SDKs and transferred to Google servers located outside of Western Australia.[133] It is not clear what this tracking information consists of and SafeWA's privacy policy is vague about the nature of this processing and the rationale behind it.

Conversely, apps that use the Google Apple Exposure Notification (GAEN) system for contact tracing could be presented as an example of good practice that ensures purpose limitation and data minimization.[134] Apps using GAEN generate random IDs (which are cryptographic tokens called rolling proximity identifiers) that change every 10-20 minutes to take account of the location of the device. When the user comes into close contact with another device with an app using the GAEN system, the two devices exchange and record their respective random IDs via Bluetooth. The mobile device will then periodically compare the random IDs it has recorded against a database of random IDs associated with a positive Covid-19 test.[135] If a match is found, then the app will notify the user that they may have been exposed to another person with Covid-19 and advised to follow the guidance of the relevant public authority such as taking a Covid-19 test and/or self-isolating for a certain period. This decentralized contact tracing system better complies with data minimization as it does not entail a central server operated by a public authority to access exposure data on the device and only has access to pseudonymized data (in the form of random IDs). Tunisia's E7mi does integrate the library for the GAEN system but this system is not actively in use with a centralized system being used instead, meaning that more sensitive data is processed by a public authority.

Was information regarding the data processing carried out by Covid apps transparent and made accessible in a convenient manner for users?

Even where the data processing carried out by Covid apps is limited to the bare minimum needed, such data processing should also be transparent. This helps to ensure that the apps are "operating according to the stated promises and objectives, subject to independent verification".[136] This requires developers to be open about the data processed by their apps, the purposes of that processing, who data may be shared with, how long it may be stored for and other relevant information (such as the use of SDKs); this information could be presented in a privacy notice available online. Transparency may also require that developers make the source code for apps open source, as this can provide a means for inspection and independent verification of the app's functions and data processing operations.

[133] See p.75 of the Tech Report.
[134] https://www.google.com/covid19/exposurenotifications/
[135] When a person enters into the app that they have received a positive Covid-19 test, then a list of the random IDs that their device has recorded in the past 14 days is communicated to a central server operated by a public authority.
[136] https://www.ipc.on.ca/wp-content/uploads/resources/7foundationalprinciples.pdf

The table below sets out the level of transparency of the Covid apps covered in this report, showing which apps have a published privacy notice, whether those notices mention the use of SDKs, and whether the source code of the app has been made open source.

Transparency of Covid Apps				
Country/Region	**App Name**	**Privacy Notice Published**	**SDKs Mentioned in Privacy Policy**	**Code Made Open Source**
Australia	COVIDSafe			
Bahrain	BeAware Bahrain			
Chile	CoronApp			
Indonesia	PeduliLindungi			
Israel	Ramzor			
Netherlands	CoronaCheck			
Netherlands	Scanner Voor CoronaCheck			
Tunisia	E7mi			
Western Australia	SafeWA			
Global	CommonPass			
Global	IATA Travel Pass			

Green = Yes, Red = No

All the Covid apps reviewed have published a privacy notice. However, none of these notices listed the SDKs embedded in their apps, the purpose of these SDKs and the data that they process. In addition, these notices were not always presented in the most convenient manner for users, for example by using a short form notice within the app providing headline information for users with the option to read the full notice. Using this approach would help to ensure that an appropriate notice is provided utilizing means that are more user-friendly, which is another important principle for implementing privacy by design.[137]

Did governments provide sufficient guidance for venue organizers required to process certain data for the purposes of contact tracing or in compliance with other public health measures?
For privacy by design, it is important that the whole of the data processing operation incorporate measures to protect personal data. This helps to "ensure that all data are securely retained, and then securely destroyed at the end of the process".[138]

This is especially relevant when certain Covid measures, such as contact tracing, require the participation of venue organizers. This is the case with SafeWA in Western Australia, where users of the app are required to scan the QR code provided by the venue organizers to register their attendance at the venue or to provide their information using the venue's manual contact register. This information is then passed on to the Western Australia Department of Health. When venue organizers are collecting this information, it is important that they do so using appropriate data processing practices. To help ensure that this is the case, the Government of Western Australia has published guidance for public venues required to maintain a contact

[137] https://www.ipc.on.ca/wp-content/uploads/resources/7foundationalprinciples.pdf
[138] Ibid.

register.[139] This guidance includes a template for paper-based registers and best practices relating to privacy.

Were Covid apps subject to a data protection or privacy impact assessment before or after deployment?

Data protection impact assessments are assessments that detail the processing operation of a system or project, identify the potential data protection risks of that system or project, and set out the mitigation measures to address those risks. A DPIA carried out before deploying a mobile app that processes sensitive data for public health purposes can be a key tool for ensuring privacy by design. Such an assessment would reveal the potential risks that a Covid app may present, and measures can be built-in and implemented to ensure the mitigation or elimination of those risks while the app is being developed. Privacy considerations are thereby embedded in the design of the app from the beginning rather than being added after the app is deployed.

For COVIDSafe in Australia, a privacy impact assessment was published on April 24, 2020, and thus before the app was launched on April 27, 2020.[140] In Western Australia, no data protection or privacy impact assessment was completed for SafeWA but an audit of the app was carried out by the Office of the Auditor General that looked at, *inter alia*, the legalities of data processed by the app being shared with law enforcement.[141] This was published in August 2021, several months after SafeWA was launched in the previous November. Apart from these two Australian apps, no other apps within the scope of this report have been subject to a data protection or privacy impact assessment carried out by the developer either before or after deployment. Without such assessments, successfully implementing privacy by design becomes potentially more difficult, resulting in users suffering privacy risks that may not have been sufficiently addressed before deployment.

Recommendation: *Those involved in the development of Covid apps should adhere to the principle of privacy by design by:*

- *Only using SDKs that process personal data necessary for the purpose of the app (i.e., contact tracing and/or displaying health information).*
- *Producing privacy notices that inform app users in clear and concise language about how their data are collected and processed, and delivering such notices in a user-friendly manner.*
- *Making the source code for the apps open source to allow for independent verification of the app's functions and data processing operations.*
- *Where the processing of personal data involves processing by public venue organizers (for example with both digital and manual contact tracing), providing guidance on how to process such data in a responsible manner that is conducive to good data protection.*

[139] https://www.wa.gov.au/government/covid-19-coronavirus/covid-19-coronavirus-contact-registers

[140] https://www.health.gov.au/sites/default/files/documents/2020/04/covidsafe-application-privacy-impact-assessment-covidsafe-application-privacy-impact-assessment.pdf

[141] https://www.parliament.wa.gov.au/publications/tabledpapers.nsf/displaypaper/4110334abb0c51edaba5b8554825872600289bbb/$file/tp+334+(2021)+report_2__safewa++application+audit.pdf (see p.7)

- *Carrying out data protection or privacy impact assessments before deployment to identify potential data protection or privacy risks and develop appropriate mitigation measures for those risks.*

Public procurement during Covid-19

As discussed in Pillar 1, during the Covid-19 pandemic many countries had to procure a number of goods and services to help combat the virus, ranging from ventilators to vaccines. Particularly during an emergency, it is important to have expedited legal processes in place to ensure the efficacy of such acquisitions so that measures and policies can be enacted effectively. Additionally, such expedited processes for public procurement should also ensure that the procurement process is ethical. More specifically, certain safeguards should be built into the expedited processes so that, while acquisitions can be made speedily, fraud, corruption, misconduct or acquisitions that are not conducive to the upholding of human rights can be avoided or mitigated.

One example of potentially unethical practices taking place in the context of public procurement during Covid-19 was identified in Israel. In May 2020, the Israeli government procured the services of a private company, J&K Experts, to manage logistics for the distribution of supplies to hospitals during the pandemic.[142] The contract was reportedly worth USD490 million and, according to the Health Ministry's head of procurement, the company was chosen due to its "rich experience in logistics".[143] However, the company itself had only formed a few years before the contract was signed and its CEO, Noam Yaacov, was a former army officer who had previously worked for the Israeli Prime Minister on procurement for military intelligence. Such circumstances may cast some doubt over the integrity of the procurement process in Israel, in particular whether the arrangement was made after genuine and careful consideration or whether it was made due to pre-existing relationships between members of the government and the service provider.

A lack of transparency can also create a similarly negative impression. Australian law requires government agencies to publish procurement contracts to the AusTender website within six weeks of them being signed.[144] However, details of the Australian government's contract with PwC, in which the consulting firm was paid USD11.4 million to provide management support for the country's vaccine program, was not published on AusTender for over eight months;[145] the contract was issued via a closed tender process, which the Department of Health stated was necessary to "protect human health".[146] Furthermore, this firm was one of several private companies that were criticized for Australia's poor rollout of Covid-19 vaccines in the summer of 2021.[147] Given the lack of transparency about these arrangements, governments will struggle to argue the legitimacy of their decision-making and instead perpetuate a perception that

[142] https://www.haaretz.com/israel-news/business/.premium-privatization-of-israel-s-covid-fight-leads-to-dubious-contracts-higher-prices-1.9101332
[143] Ibid.
[144] Rule 7.18 of the Commonwealth Procurement Rules (December 2020), https://www.finance.gov.au/sites/default/files/2020-12/Commonwealth%20Procurement%20Rules%20-%2014%20December%202020.pdf.
[145] https://www.innovationaus.com/pwc-paid-1m-per-month-for-vaccine-rollout-work/
[146] Ibid.
[147] https://www.theguardian.com/society/2021/apr/11/australias-covid-vaccination-relying-on-opaque-private-contracts-worth-millions

contracts are being rewarded for potentially nefarious or unethical purposes. This could take the form of, for instance, unequal treatment of suppliers.

In Tunisia, the Observatory of Emerging Diseases entered into a public-private partnership with a Tunisia-based start-up called WizzLabs to develop E7mi, the national contact tracing app. However, despite the involvement of a private enterprise in the development of the app, the Tunisian government has shared no information on the nature of the arrangement. Access Now, a human rights organization, made an information request to the government in July 2020 regarding the consultation between the Health Ministry and the National Authority for the Protection of Personal Data on the compliance of E7mi with Tunisian data protection law and a copy of the contract between Wizzlabs and the Health Ministry.[148] Such information would give an indication as to whether the public procurement process took into account the requirements of data protection law to ensure that Tunisians' personal data are used responsibly and safely by the app even with the involvement of a private company in the app's development. For example, it could reveal whether Wizzlabs is barred from accessing personal data processed by the app or using software developer kits that share data with third parties for purposes other than public health. However, in breach of Tunisian law, Access Now received no response to its request, including no notice showing the legal grounds on which such information could be withheld.[149] This is another example of opaque procurement processes preventing governments from being held to account for contracts with private sector entities that may undermine human rights.

Recommendation: *Governments acquiring goods or services from private sector entities should be legally mandated to ensure the fair and equal treatment of all potential suppliers and that any resulting arrangements do not undermine human rights or the general interests of the populace. Such a legal framework should also require the details of these arrangements be made available to the public.*

Unintended Consequences

Covid certificate fraud and app design: the Netherlands

Fraud is a widely observed phenomenon and includes amateurish attempts to fraudulently obtain large quantities of fully functional Covid certificates. As these instances of fraud were relatively well reported on in the Netherlands, the case of that country is described and analysed here. It is considered as there is sufficient information, allowing for a representative illustration of the situation globally.

Likely partially due to the misinformation and conspiracies surrounding Covid-19, there were cases where people attempted to obtain fraudulent QR codes to access venues or travel. In the Netherlands, the likely number of fraud cases runs into the tens of thousands via a variety of methods, including people selling "home-made" fake QR codes, mostly online, which did not

[148] https://www.accessnow.org/to-safeguard-privacy-tunisia-must-be-transparent-on-tech-used-to-fight-COVID-19/
[149] See Article 14 of Organic Law No. 2016-22: https://www.bct.gov.tn/bct/siteprod/documents/Loi_2016_22_en.pdf.

grant the user access when the code was scanned. There were also tens of thousands of functioning fake QR codes created in a number of ways. Firstly, some medical practitioners registered several dozen unvaccinated people as vaccinated, who could then obtain a vaccination certificate and QR code. Similar fraud was committed by public health authority employees.[150]

In another case, a government-subsidized private testing firm had a number of problems. The firm, which had 13 locations (ten in the Netherlands, three in Belgium), suffered a data leak and the personal information of 60,000 people was made publicly available. The information, all belonging to people who had been tested by the firm, included their full name, email addresses, phone numbers, social security number, passport number, and positive/negative test results. Accessing the personal data of any of these 60,000 people made it possible to create a fully functional, yet fraudulent, QR code.
The front end of the website communicates with the Google database Firestore, which could be accessed through any browser. Significantly, this information could not only be viewed but also manipulated. The private testing firm concerned was an official partner of the Ministry of Public Health, Welfare and Sport and the CoronaCheck app, meaning that a QR code could be created for the fake negative tests. In July 2021, this led to a temporary shutdown of Covid-19 testing for travel and venue access at that firm.[151,152] Initially, the fraudulent QR codes could not be excluded from the system.
Different app design, such as in Belgium, did allow for more granular exclusions of specific QR codes. This was the case in Belgium, where people who tested positive for Covid-19 could not generate a normal QR code in the 11 days following the test, and if the positive test was a PCR, a recovery certificate was automatically available afterwards.[153] From a public health point of view, the effectiveness of the Dutch app was compromised as it would not prevent infected individuals from entering public spaces and therefore possibly spreading the virus. The Dutch app seems to have been developed assuming that people would act in good faith. It should be noted, however, that there are no widespread reports of people knowingly using their fraudulent Covid certificate while being infected. Notably, the Belgium Covid-19 app is out of the scope of this report, and thus no assessment can be made about the trade-off between privacy and the ability to (temporarily) disable QR-codes.

In November 2021, the Ministry of Public Health, Welfare and Sport announced that they had found a way to exclude known fraudulent QR codes from the app, yet they have not communicated how this was achieved, claiming the information might be used by criminals. There are some conflicting reports on how it was done. The Ministry first indicated that the CoronaCheck app scans for known fraudulent codes, while the Ministry website states that these known fraudulent codes are not in the CoronaCheck app itself, but instead loaded into the CoronaCheck scanner app, which was mandatory for venues to use to confirm the validity of QR codes.[154,155] The screen of the scanner app turns green when someone can enter, and red if they cannot. In November 2021, the Ministry had identified 60 QR codes as fraudulent. As the number of fraudulent codes likely ran at least into the tens of thousands, this number represents a fraction of the total number of fraudulent codes. This approach, and the absence of transparency on the part of the government, poses a significant risk both to public trust in the

[150] https://www.parool.nl/amsterdam/doktersassistenten-aangehouden-voor-handel-in-valse-vaccinatiebewijzen~b1d8dee7
[151] https://twitter.com/danielverlaan/status/1416673022023458816?lang=en
[152] https://www.rtlnieuws.nl/nieuws/nederland/artikel/5242193/valse-coronacheck-bewijzen-datalek-testcoronanu
[153] https://www.uzgent.be/wat-moet-ik-doen-na-een-positieve-test
[154] https://coronacheck.nl/nl/faq/7-8-wat-gebeurt-er-met-qr-codes-waarmee-gefraudeerd-is/
[155] https://www.nu.nl/tech/6168028/ministerie-doet-aangifte-tegen-testaanbieder-om-valse-vaccinatiebewijzen.html

app and to its ability to function effectively as a public health measure. In response to an inquiry addressed to the Ministry, they indicated that there were around 1,500 known functioning fraudulent QR codes and that an unspecified number of these are known by the app – not the scanner. To the follow-up question on how this was achieved, perhaps through individually loading known fraudulent codes into the app when it updates, or more substantial changes to the app design, the Ministry replied that they had done neither, but that they were unable to share what had been done to prevent the use of fraudulently acquired QR codes.

The Ministry of Public Health emphasizes that it is important for venues to also check someone's passport or ID card, as well as the info on the CoronaCheck app beyond the QR code: name, type of vaccine, date of birth, and type of validity (short-term, based on a negative test, or longer, based on vaccination or recovery status). This conflicts with the data minimization principles that were originally part of the app design. In addition, many of the fraudulent QR codes – given out by medical professionals or public health employees, or created from the data leaked from the large testing provider – do show the correct personal information of the person with the fraudulent code, and therefore this diminished privacy has probably not resulted in restoring the ability of the immunity passport to contribute to public health efficacy.

Recommendation: *Anticipate attempts at fraud and ensure adequate vetting of all parties involved, including private sector partners. Under the principle of privacy by design, enable the removal of fraudulently obtained certificates, allowing this process to be integrated into the privacy statement in a transparent manner.*

Access to public spaces

As discussed in Pillar 1, governments introducing measures to address a public health emergency should ensure that such measures are based on scientific evidence to strengthen the case for their necessity. However, another important issue that should also be considered is that such measures, even when they may be necessary from a scientific perspective, ought not to result in unfairly excluding large sections of society.

This consideration can be applied to the introduction of immunity passport apps. In particular, governments should question whether the introduction of immunity passports is aligned with vaccine coverage and availability so as to avoid unfairly excluding certain groups. In other words, it should be asked whether it would be unfair to introduce immunity passports and make their use mandatory to access public spaces if (i) not many people have been vaccinated at that point, and/or (ii) vaccines are not widely available to the general public.

Below is a table of the countries that released immunity passport apps, including whether their use was mandatory, along with the respective vaccine coverage and availability in each country.

Immunity Passports and Vaccine Coverage					
Country	App	Launch Date[156]	Mandatory	Availability of Vaccine (at	Population Vaccinated (at

[156] This date is either when the app was launched or when it first introduced immunity passport features.

				Date of App Launch)[157]	Date of App Launch)[158]
Bahrain	BeAware Bahrain	Feb 2021	No	Universal	18%
Indonesia	PeduliLindungi	Sept 2021	Yes	Vulnerable + some others	19%
Israel	Ramzor	Feb 2021	Yes	Universal	37%
Netherlands	CoronaCheck	June 2021	Yes	Vulnerable + some others	34%

In Indonesia, people were required to show their vaccination status on the PeduliLindungi app to enter supermarkets in September 2021. At that time, vaccines were available for vulnerable groups (i.e., key workers, clinically vulnerable people and elderly people) and there was only limited availability for the wider population. In addition, only 19% of the population was vaccinated when the vaccination status features were first introduced in PeduliLindungi. As such, making the immunity passport mandatory to access essential goods from a supermarket when much of the population cannot be vaccinated unfairly excludes those people from accessing such essential goods.

A similar point could be made regarding Covid-19 tests, the results of which can be shown with some immunity passport apps. If testing is not widely available to the general population despite a negative test result being a condition for entry into public venues, then this may result in the exclusion of large sections of society. Countries like Israel and the Netherlands released immunity passport apps that allow users to show either their vaccine status or a negative test result (as well as evidence of natural immunity). When Ramzor was released in February 2021, Covid-19 testing in Israel was available to the general public.[159] At the time of the release of CoronaCheck in the Netherlands in June 2021, testing was available to anyone showing symptoms.[160] Thus, where a negative test result is required for entry to public venues, testing should be made easily available so that as many people as possible can access public spaces and not be unfairly excluded. Notably, there have been sporadic reports of people deliberately infecting themselves with Covid-19 in order to later get a recovery certificate to access public spaces. (See the case of a Czech woman who died of Covid-19.)[161] This further underlines the importance of public awareness campaigns by the government with broad coalitions to inform people about the effectiveness and safety of vaccines, instead of applying immunity passports as nudging to motivate people to get vaccinated.

Additionally, providing people with a choice between using technological or non-technological means could also be an effective way of avoiding the unfair exclusion of people from public spaces. For instance, in the Netherlands, there is an option to present a Covid test or vaccination status either through CoronaCheck or via paper records.[162] Making the use of a

[157] "Vulnerable + some others" means key workers, clinically vulnerable people and elderly people.
[158] This is the share of the population with a complete initial protocol at the end of the same month when the immunity passport app/features were launched: https://ourworldindata.org/explorers/coronavirus-data-explorer?zoomToSelection=true&time=2021-02-28&facet=none&pickerSort=asc&pickerMetric=location&Metric=People+vaccinated+%28by+dose%29&Interval=7-day+rolling+average&Relative+to+Population=true&Color+by+test+positivity=false&country=BHR~IDN~ISR~NLD
[159] https://ourworldindata.org/grapher/COVID-19-testing-policy?time=latest
[160] Ibid.
[161] https://www.bbc.com/news/world-europe-60050996
[162] https://www.government.nl/topics/coronavirus-COVID-19/covid-certificate/proof-of-vaccination

technological measure such as a mobile app mandatory is better justified if that measure is necessary for the purpose. But if that same purpose can be fulfilled through non-technological means, like physical records or documents, then there ought to be a choice between the two means. This is especially important for those countries where there may be wide differences in digital access between different areas or populations; those with less digital access, for example due to poor internet infrastructure, can take advantage of the manual alternatives and still comply with the relevant restrictions.

Recommendation: *Governments should ensure that public health measures which are mandatory to follow during a public health emergency are coupled with the availability of the necessary resources and facilities so that people can comply with such rules and not be unfairly denied access to society.*

Appendixes

- Appendix 1: Summary of Insights and Recommendations from Phase 1 of the Covid App Project
- Appendix 2: Covid Apps – Key Technical Features (Phase 1)
- Appendix 3: Technical Review (Phase 2)

Appendix 1: Summary of Insights and Recommendations from Phase 1 of the Covid App Project

For Phase 1 of the Covid App Project, research was carried out by six civil society organizations: ALT Advisory (South Africa), Internet Democracy Project (India), InternetLAB (Brazil), Karisma (Colombia), SMEX (Lebanon), and United for Iran. AWO, a data rights agency, provided coordination support.

This research resulted in a report containing an assessment of the Covid-19response in six countries: Brazil, Colombia, India, Iran, Lebanon and South Africa, based on three pillars. These are: How effective contact tracing apps have been from a public health perspective (Pillar 1); How contact tracing apps interact with structural, institutional and legal infrastructure (Pillar 2); and How contact tracing apps are experienced by vulnerable and historically marginalized populations (Pillar 3).

The report for Phase 1 identified a number of insights and recommendations that may foster better protect marginalized and vulnerable groups during public health crises, bolster human rights, democracy, and rule of law, and strengthen ongoing and future pandemic responses. These insights and recommendations are also relevant for Phase 2 of the project as they concern both contact tracing apps and immunity passport apps.

Insights

Pillar 1 - Public Health Efficacy of the Covid-19 Response

1. Contact tracing apps and technology-based alternative measures were often deployed in countries with poor or unequal access to the internet and mobile technology

Many governments introduced technological measures in response to Covid-19 despite the pre-existing disparities regarding internet access and mobile technology adoption. The importance of this problem cannot be understated since unequal access to smartphone technology can "exacerbate existing inequities and raise ethical concerns."[163] Furthermore, by making social security services available predominantly through online platforms, vulnerable communities that are more likely to have poor internet access and no mobile devices may be deprived of vital assistance.

2. Apps were often disconnected from the broader public health response and affected by low uptake

The fate of contact tracing apps is closely tied to an uncoordinated overall pandemic response. In Brazil, Coronavirus SUS is largely disconnected from the rather sporadic public health strategy, and the federal government has not given priority to using its data effectively. In Colombia, CoronApp was one of many technological measures that were not aligned with the needs of the public health system, which is especially evident in the lack of data sharing between the National Institute of Health and municipal entities. In South Africa, digital rights activists have commented that the adoption of a contact tracing app is merely a box-ticking

[163] Nature. (January 21, 2021). Tracking and promoting the usage of a COVID-19 contact tracing app. Available at: https://www.nature.com/articles/s41562-020-01044-x.

exercise to show that the South African government engages in tech-based responses to the pandemic.

3. Multiple and multipurpose apps were deployed

In many countries, different contact tracing apps proliferated. In India, there are over 70; in Brazil, at least eight smartphone apps were introduced by state governments with functionalities beyond contact tracing, such as providing remote healthcare. In Colombia, CoronApp – the only national contact tracing app – is accompanied by several regional apps, a consequence of limited inter-institutional coordination and a decentralized public health system. The array of Covid-19 official contact tracing apps in these countries is possibly diluting their overall adoption, although in India's case this is mitigated to a certain extent by greater investment in promoting the Aarogya Setu app, whose use is mandatory in certain instances.

4. Alternative measures often had a greater public health impact than the apps

While contact tracing apps attract attention and public debate, alternative measures often have greater reach. In the early stages of the pandemic, for several months before the launch of COVID Alert SA, South Africa mainly relied on mass screening, targeted testing and lockdown measures. This involved mobilizing 28,000 health workers to screen over seven million people in May 2020, which helped maintain positive cases at around 3%. In India, the first national lockdown introduced in March 2020 forced over a billion people to quarantine, compared to the 120 million people who downloaded Aarogya Setu. Based on these numbers and data analyzed by MIT, it can be argued that lockdowns have done more to suppress the virus than contact tracing apps.

Pillar 2 - Increased Social Control

1. Legal frameworks: weakening of checks and balances to combat Covid-19

To respond to Covid-19, a number of countries around the world expanded their emergency powers. In fact, since the World Health Organization (WHO) designated Covid-19 a global health emergency, over 100 countries have declared a state of emergency. However, recourse to such emergency laws in the countries studied is limited existing extraordinary powers are used in order to tackle the pandemic.

   a. Limited recourse to emergency laws which facilitate the securitization of Covid-19 response

During the period of study, not all the countries of focus declared a national emergency. For those that did, the legal basis for implementing various measures derived from specific provisions within the country's constitution or legal framework. This typically means that, subject to certain conditions and rules, powers can be exercised by the state whilst derogating from the usual human rights standards. This was the case in Colombia where a state of emergency can only be declared for up to 30 days with the proviso that the Constitutional Court may judicially review decisions made during that timeframe. However, a state of

emergency can negatively impact certain vulnerable communities, especially where the measures implemented encode and exacerbate existing discriminatory practices.

b. Extended use of extraordinary powers and increased surveillance

For those countries that did not declare a state of emergency, ordinary legislative provisions together with extraordinary powers were relied on. This differs from declaring a state of emergency given that the basis of such powers lies in pre-existing legislation, typically public health laws, permitting certain measures to be implemented without necessarily being tied to a type of emergency. This may not always be in accordance with explicit provisions in the constitution or legal framework, and therefore gives rise to the possibility that broad powers are exercised without the appropriate checks and balances in place.

2. The countries of focus have nascent, sometimes unenforced, data protection regimes

In the countries of focus, comprehensive data protection laws are either not yet in force, are still going through the legislative process, or simply do not exist. South Africa falls into the first category, with the substantive provisions of the Protection of Personal Information Act of 2013 only becoming enforceable beginning July 1, 2021. In Brazil, the General Data Protection Law was delayed until August 2021, and a similar situation exists in Lebanon where Law No. 84 of 2018 on Electronic Transactions and Personal Data is yet to be implemented. In India, a joint parliamentary committee has not to date submitted its report on the 2019 Personal Data Protection Bill. There is currently no data protection law in Iran. Colombia stands out as the only country with an existing law, although these rules have been relaxed during the pandemic to allow public authorities to collect personal information without the usual restrictions. In general, stronger data protection regimes may strengthen oversight across the countries in question.

a. Increased and non-transparent data sharing between public authorities

Public authorities collecting and sharing data in response to the pandemic is common across governments around the world. The main reason given is to facilitate and approve applications for internal travel whilst quarantine measures are in place. This involves combining pre-existing datasets as well as those datasets generated specifically for Covid-19. However, the absence of comprehensive data protection laws or other regulatory checks gives rise to function creep and adverse impacts on certain vulnerable communities through the sharing of sensitive personal data with law enforcement and restricting the movement of those typically unable to access online platforms to apply for travel permissions.

b. Rise of public-private partnerships and lack of transparency

Governments often try to leverage their relationships with private sector entities to achieve various policy ends. Covid-19 is no exception; many governments choose to use the Google/Apple Exposure Notification system to build their digital contact tracing apps; some countries look to telecommunications companies to acquire data to create heat maps and track the spread of the virus; governments also install camera systems to monitor compliance with

quarantine rules, thus expanding the state surveillance apparatus. However, often these partnerships are cloaked in secrecy or, in the context of Covid-19, exploit the emergency context to escape the usual regulatory constraints that serve to ensure that rights are protected.

3. A lack of public trust and awareness affects contact tracing apps

Adoption of contact tracing apps is hampered by either a lack of public trust or public awareness in all of the countries under review. Part of this stems from poor campaigning around the app, as is the case in South Africa where the absence of focused and targeted communications from the government contributed to public confusion around COVID Alert SA. Additionally, some apps suffer from concerns around surveillance and privacy. In Colombia, for instance, there is a history of abuse of surveillance powers by law enforcement and intelligence services, impacting journalists, opposition leaders, judges, and human rights activists.

4. Impact on vulnerable communities
    a. Discrimination against marginalized groups

In Punjab, India, people were encouraged to report lockdown violators to public authorities via the Cova app, which contains a feature that allows users to report mass gatherings and inter-state travelers in their area. However, this can have grave consequences for marginalized groups, with members of society asked to carry out surveillance on behalf of the state without the commitments to equality that states must usually follow. Indians were thus given the opportunity to unfairly penalize certain individuals or even whole groups.

    b. Suppression of protests

Protests broke out across Colombia in reaction to the insufficient aid provided by national and local governments to mitigate the problems invoked by lockdowns and other Covid-related measures. In Bogotá and Medellín, the police used disproportionate force to suppress protestors, impacting children, the sick, and older people in particular.

In Lebanon, protests escalated in response to the government's alleged mishandling of the economic crisis during the pandemic. Protests were also fueled by the lack of government support during national lockdowns, exacerbating the downturn experienced by many. Demonstrations led to numerous casualties during clashes with security forces as authorities attempted to suppress protests, including during the national lockdown that began in January 2021.

Pillar 3: Equal Access to Society

1. The tech-based Covid-19 response exacerbated the digital divide and inequalities

The disparities in internet access and the use of mobile technology, as discussed in Pillar 1, also have an impact on individuals' access to society during the pandemic. This proves to be a

critical issue since unequal access to such resources can "exacerbate existing inequities and raise ethical concerns." Furthermore, by making social security services available predominantly through online platforms, vulnerable communities, many of whom lack adequate internet access and have few mobile devices, may be deprived of essential services, as was the case in Colombia. However, even where platforms are physically accessible, their design can have negative implications that extend beyond vulnerable communities. For instance, South Africa's contact tracing app is only available in English despite it being only one of many local languages.

2. Acute impact on vulnerable communities
    a. Migrants and refugees

While Covid-19 measures, particularly national lockdowns and stringent border controls, impact whole populations, migrants and refugees are at a heightened risk of exclusion or discrimination. However, ensuring that vulnerable communities are protected from these risks is not always well-managed, as seen in the focus countries. Many people struggle with travel restrictions, especially when permission to travel can only be obtained via digital platforms. Some even have difficulties in finding housing in the midst of national lockdowns, as was the case in Brazil.

    b. Informal settlements

Covid-19 has intensified the challenges facing rural people and those in informal sectors of the economy. In South Africa where, apart from the threat of the virus itself, insufficient water supply and overcrowding are "but a few of the many challenges faced by many indigent people." This is in addition to the contentious use of quarantine camps, where migrants were kept in isolation for 14 days without being tested for Covid-19 and denied the opportunity to self-isolate. In May 2020, AfriForum (a civil rights organization) succeeded in a legal challenge against the South African government regarding these camps, declaring that they should be closed immediately.

Recommendations

Pillar 1: Public Health Efficacy of COVID-19 Response

Coordinated response and inclusion of vulnerable populations

- Develop a unified government response to the Covid-19 pandemic, taking into account both national and local-level government bodies.
- Maintain access to vital services for vulnerable populations (particularly refugees and migrant workers).
- Provide increased aid to people in need in a more efficient manner and limit the role of the army to prevent the securitization – or even perception of securitization – of the public health response.
- Strengthen cooperation and coordination between the public and private sector to ensure hospital preparedness.

Communication strategy

- Improve communication with the media. Content should be scientific and delivered in a professional manner to increase public awareness and education.
- Encourage the media to engage with other sectors, specifically academia, the technical community, and civil society to ensure the publication of information that is true, accurate, and fair.

Pillar 2: Increased Social Control and Pillar 3: Equal Access to Society

Regarding applications and technology to fight the pandemic

- Provide clear information regarding the type of data collected and for what purpose, where and for how long data will be stored, with whom the data will be shared and for what purposes, as well as the security protocols for all of these functions.
- Approach application development using a privacy-by-design framework.
- Clearly frame data sharing practices between different government entities as well as with the private sector.
- Release into the public domain the terms of the partnership for all apps developed through a public-private partnership.
- Remove requests for location data from any contact tracing applications to protect privacy.
- Publish more detailed privacy policies (written in all local languages) and explicitly name any third parties who have access to data.
- Make all existing Covid-related apps open source on all platforms. By making the server-side codes publicly accessible and auditable, people can collaborate, check the codes for vulnerabilities, and start a peer-review system.
- Make all Covid-related apps purely voluntary across all sectors, and ensure that non-participating individuals are not penalized, or denied access to any service, public or private.
- Offer a clear and easy-to-access option to delete an account and information from the app, as well as from the server.
- Minimize the amount of data collected to what is strictly necessary, particularly personal or identifiable data; this includes eliminating the need for GPS location.

Oversight and review mechanisms

- Oversight bodies must be involved from the outset, prior to the deployment of data-driven technological tools to ensure the protection of individuals' rights.
- Regular monitoring is also necessary to ensure proportionality of the measures in the long run.

Recognition of the impact of Covid-19 responses on various rights

- The impact of Covid-19 responses on various rights, including their potential to exclude and discriminate against vulnerable communities and their impact on the freedom of the press, should be assessed and evaluated by governments, taking into account the

legal framework that guides the government's approach. These evaluations should be conducted over the short-, medium- and long-term in a manner that reveals the successes, challenges, and mistakes of the policy approaches chosen.

- In future crises, human rights impact assessments should inform the legal framework, including guidelines for states of emergency and states of disaster, indicating what is necessary and justifiable in any given situation.

Appendix 2: Covid Apps – Key Technical Features

The tables in this Appendix provide details of key technical features of the Covid-related apps covered in the present report.

BeAware (Bahrain)	
Description	BeAware Bahrain is the official contact tracing app for the Kingdom of Bahrain. The app helps the government's efforts to contain the spread of Covid-19 through digital contact tracing, digital Covid-19 immunity passports, and other related services. It is available for iOS and Android devices.
Developer(s)	Information & eGovernment Authority Bahrain (public entity)
Functionality	Contact tracing and immunity passport
Privacy Policy	Yes
Code Transparency	The app code is obfuscated and is not open source
Downloads (Google Play Store)	Over 1 million
Data Processed	Passport number, location data, user ID, test results and vaccination status[164]
Notable Data Access and Sharing	App Permissions: • Requests access to location data (when the device is in motion) to provide location-based services, e.g., to provide a map of nearby testing facilities. • Requests access to the calendar to create, modify and delete vaccination appointments. • Requests access to the device storage and camera to scan documents and take facial images during registration.
	Third Party SDKs and Software Libraries: • *TransistorSoft* – This is a software library providing geolocation services. It relies on motion sensors to turn the location plugin on or off. • *AltBeacon* – This library is used to manage Bluetooth beacons. For example, it can trigger notifications whenever new devices are available. • *Google Firebase* – This SDK is used for tracking a range of activities within the app and monitoring app status.[165]
	Servers Contacted: • Amazon Web Services (located in the United States) • Google (located in the United States) • TransistorSoft
Other Information	One of the packages from the TransistorSoft library contains Chinese characters which cannot be translated due to the use of custom encoding. Plus, data sent to TransistorSoft servers are not encrypted.

[164] The privacy policy of BeAware does not specify which data are being collected and sent by the app.
[165] See Tech Report (p.43) for full list of events tracked using Google Firebase.

CommonPass (Global)	
Description	CommonPass is an application developed by the Commons Project, a non-profit organization based in Switzerland. It permits users to privately share their health status, i.e., proof of vaccination and/or negative Covid-19 test. It is compatible with vaccine administrators or testing laboratories that provide SMART Health Cards, which provide information using QR codes. Once users test negative or are vaccinated, they scan the issued QR code with the app. It can be used for travelling to specific places, or as a general-purpose certificate. It is available for iOS and Android devices.
Developer(s)	The Commons Project Foundation and the World Economic Forum
Functionality	Immunity passport
Privacy Policy	Yes
Code Transparency	The app code is not obfuscated and is not open source
Downloads (Google Play Store)	Over 100,000
Data Processed	Test results, vaccination history, laboratories where the user has been tested, type of tests, email, IP address, unique device identifier, device type, type of mobile users, operating system, how many times a user uses the app, crash and bug information, and how users access and use the app.
Notable Data Access and Sharing	App Permissions: • Requests access to the device camera to allow for QR code scanning. • Requests access to network information and the device's network connections (i.e., the internet) to deliver the app's functionality.
	Third Party SDKs and Software Libraries: • *Bugsnag* – This is a tracking library for monitoring application stability using crash reports recording activity such as network connectivity, Bluetooth status, low battery and turning the screen on and off. • *NewRelic* – This is a library providing developers with information on app crashes and other events for service improvement.
	Servers Contacted: • Google (located in the United States) • Amazon Web Services (located in the United States) • Akamai (located in the United States) • Squarespace (located in the United States) • Fastly (located in the United States) • NewRelic (located in the United States)
Other Information	The app uses two software libraries collecting information for app performance and service improvement (Bugsnag and NewRelic), which seems excessive.

CoronApp (Chile)	
Description	CoronApp is an official app from the Chilean Ministry of Health that allows citizens to self-diagnose based on symptoms and receive a risk classification, receive official notifications from the Ministry of Health, deliver and receive information related to the pandemic evolution and status, report and inform about high-risk events or behaviors observed, and ask for or offer help to neighbours. It is available for iOS and Android devices.
Developer(s)	Gobierno Digital
Functionality	Self-diagnosis and information dissemination
Privacy Policy	Yes
Code Transparency	The app code is obfuscated and is not open source
Downloads (Google Play Store)	Over 100,000
Data Processed	Passport ID, email, phone number, full name, age, province, health data (i.e., symptoms), images, physical address, and GPS coordinates
Notable Data Access and Sharing	App Permissions: • Requests access to location data to provide the relevant services within the app, e.g., to locate nearby health centers. • Requests access to the device storage to access photos stored on the device.[166]
	Third Party SDKs and Software Libraries • *Trust Fall* – This is an SDK that can check whether a device is rooted to ensure that the app does not run on these devices.[167] • *Google Firebase* – This SDK is used for tracking a range of activities within the app and monitoring app status.
	Servers Contacted: • Amazon Web Services (located in the United States) • Cloudflare (located in the United States) • Facebook[168] (located in the United States) • Google (located in the United States)
Other Information	The app uses a Cloud Application Framework called HerokuApp that allows developers to build and deploy apps; its URL leaks information about the services allowed for the app, giving rise to potential security breaches.[169]

[166] As stated in the Tech Report (p.66), the app accesses the device's storage for largely unknown purposes, though access to photos can be presumed given that one of the features of the app (requesting help from neighbours) allows users to share photos.
[167] A rooted Android device is one where the user has accessed the root (lowest) level of the operating system, giving the user the ability to change the operating system, tweak the hardware or even unlock the phone from its carrier. See https://www.pcmag.com/encyclopedia/term/android-rooting.
[168] This server is contacted to use the WhatsApp API.
[169] See p.67 of the Tech Report for more information.

CoronaCheck (Netherlands)	
Description	CoronaCheck is an official app from the Ministry of Public Health, Welfare and Sport of the Netherlands. It is used to provide a digital certificate (in form of a QR code) for citizens who either have tested negative for COVID-19, have been infected with the virus before and recovered, or are currently vaccinated. The QR code contains both a Coronavirus pass (issued by the Dutch government) and the EU Digital COVID Certificate (ECC). It is available for iOS and Android devices.
Developer(s)	Rijksoverheid
Functionality	Immunity passport
Privacy Policy	Yes
Code Transparency	The app code is not obfuscated and is open source
Downloads (Google Play Store)	Over 5 million
Data Processed	IP address, social security number and full name
Notable Data Access and Sharing	App Permissions: • Requests access to device camera to scan QR codes.
	Third Party SDKs and Software Libraries: • *Google Firebase* – This SDK is used for tracking a range of activities within the app and monitoring app status. • *Rootbeer* – This library is used to warn users when they are using a rooted device.[170] • *Google Mobile Services* – This is used as a support library and its tracking services are not activated.
	Servers Contacted: • Prolocation (located in the Netherlands) • Intermax (located in the Netherlands)
Other Information	The Dutch government provides specific information for researchers on how the app works.[171]

[170] A rooted Android device is one where the user has accessed the root (lowest) level of the operating system, giving the user the ability to change the operating system, tweak the hardware or even unlock the phone from its carrier. See https://www.pcmag.com/encyclopedia/term/android-rooting.
[171] https://coronacheck.nl/en/faq/7-1-onderzoek-hoe-weten-we-of-coronacheck-werkt/.

COVIDSafe (Australia)	
Description	COVIDSafe is a contact tracing app approved by the Australian government. When two devices using the app come into close contact, temporary IDs and encrypted tokens are shared and used to alert users who may have been exposed to Covid-infected persons. It supports the manual processes carried out to identify those who have been in close contact with someone with Covid-19. It is available for iOS and Android devices.
Developer(s)	Australian Department of Health
Functionality	Contact tracing
Privacy Policy	Yes
Code Transparency	The app code is not obfuscated and is open source
Downloads (Google Play Store)	Over 1 million
Data Processed	Username, age range, mobile number, postcode and email address
Notable Data Access and Sharing	App Permissions: • Requests access to location data to support the contact tracing features via Bluetooth.[172]
	Third Party SDKs and Software Libraries: • *Google Firebase* – This SDK is used for tracking a range of activities within the app and monitoring app status. • *Atlassian* – This is a tracking library that is used to provide information when users request technical support, e.g., to report an issue.
	Servers Contacted: • Google (located in the United States) • Amazon Web Services (located in the United States) • Squizus (located in the UK) • Akamai (located in the United States) • Incapsula (located in the United States)
Other Information	While the app's privacy notice states that diagnosis information is sent to the National Data Store, the endpoint server used for this process belongs to Atlassian, meaning diagnosis information (which includes email addresses) may be shared with this third party.

[172] This location permission is required to access Bluetooth functionalities on Android, and so GPS coordinates or movements are not recorded. See p.77 of the Tech Report.

E7mi (Tunisia)	
Description	E7mi is the official contact tracing app in Tunisia. It identifies and alerts users who may have had contact with others infected with COVID-19. It is available for iOS and Android devices.
Developer(s)	Tunisia's Observatory of Emerging Diseases (ONME) and Wizzlabs (IT services start-up headquartered in Tunis)
Functionality	Contact tracing
Privacy Policy	Yes
Code Transparency	The app code is not obfuscated and is not open source
Downloads (Google Play Store)	Over 100,000
Data Processed	Phone number and dynamic device identifiers
Notable Data Access and Sharing	App Permissions: • Requests access to location data (including background location) to support the contact tracing features via Bluetooth.[173]
	Third Party SDKs and Software Libraries: • *Apollo GraphQL* – This library is used for tracking activity within the app.
	Servers Contacted: • Tunisian Internet Agency (located in Tunisia) • Telefonica (located in Spain) • Akamai (located in the United States) • Cloudflare (located in the United States) • Google (located in the United States)
Other Information	Whilst the app integrates the library for the Google-Apple Exposure Notification system (for decentralized contact tracing), this functionality is not actually in use and a centralized protocol is used instead.

[173] As stated on p.90 of the Tech Report, the use of background location seems excessive for this purpose as only access to fine location is needed to access Bluetooth functionalities on Android.

IATA Travel Pass (Global)	
Description	The IATA Travel Pass Initiative allows users to safely convey Covid-19 results or certificates to participating governments and airlines prior to travel. It uses technology from Everynm, a platform focused on verifiable credentials. It is available for iOS and Android devices.
Developer(s)	International Air Transport Association and Evernym
Functionality	Immunity passport
Privacy Policy	Yes
Code Transparency	The app code is not obfuscated and is not open source
Downloads (Google Play Store)	Over 100,000
Data Processed	Facial photographs, facial video recording, passport information, flight booking reference, test results, proof of vaccination
Notable Data Access and Sharing	App Permissions: • Requests access to location data to provide the user with information about nearby testing laboratories. • Requests access to the device camera to capture facial images of the user for passport identification verification. • Requests access to the device storage so that the app can store persistent files relevant to the services and functionality it provides.[174]
	Third Party SDKs and Software Libraries: • *Google Firebase* – This SDK is used for tracking activity within the app to change the behavior and appearance of the app without pushing an app update and to customize the app based on the user's profile, including providing the local time or to provide different health credential test types depending on the issuing country. • *Google Cloud Audit Logs* – This is a library used to record administrative activities for security, auditing and compliance purposes.
	Servers Contacted: • Amazon Web Services (located in the United States) • Cloudflare (located in the United States) • Google (located in the United States)
Other Information	The app temporarily stores sensitive information in the shared media folder of the device, potentially making it accessible to other apps that request access to the device storage.

[174] The privacy policy for the app states that data is "stored encrypted to the digital wallet on [the] device." See https://www.iata.org/travelpass-privacy/.

PeduliLindungi (Indonesia)	
Description	PeduliLindungi ("CareProtect") is the Indonesian government's contact tracing app designed to assist tracking and stopping the spread of Covid-19. It also includes a vaccination status feature. It is available for iOS and Android devices.
Developer(s)	The Ministry of Communication and Information of the Republic of Indonesia
Functionality	Contact tracing and immunity passport
Privacy Policy	Yes
Code Transparency	The app code is obfuscated and is not open source
Downloads (Google Play Store)	Over 50 million
Data Processed	Facial photographs, facial video recording, passport information, flight booking reference, test results, proof of vaccination
Notable Data Access and Sharing	App Permissions: • Requests access to location data (including background location) to track the user's movements and notify them when they enter certain geographical areas. • Requests access to device camera to take photographs for self-assessments and to scan QR codes. • Requests access to the device storage to store files relating to the services and functionalities provided by the app.
	Third Party SDKs and Software Libraries: • *Google Firebase* – This SDK is used for analytics and tracking crash reports. • *String Care* – This is a library to obfuscate the app's code when the app is running.
	Servers Contacted: • Akamai (located in the Netherlands) • Google (located in the United States) • Alibaba (located in China)
Other Information	The privacy policy for the app admits that location data is collected via a third-party SDK and is in fact shared with that third party.[175]

[175] https://www.pedulilindungi.id/kebijakan-privasi-data?lang=en

Ramzor (Israel)	
Description	Ramzor is an app developed by the Israeli Health Ministry to allow users to show their Green Pass, which is a document that allows vaccinated people (and those recovered from Covid-19) to access places of worship, gyms, museums, and facilities otherwise restricted. It is available for iOS and Android devices.
Developer(s)	Israeli Ministry of Health
Functionality	Immunity passport
Privacy Policy	Yes
Code Transparency	The app code is obfuscated and is not open source
Downloads (Google Play Store)	Over 1 million
Data Processed	Location data, business name, date, time of entry, time of departure, identity information and pass validity
Notable Data Access and Sharing	App Permissions: • Requests access to the phone state (which includes information about the cellular network used, the status of ongoing calls, and a list of phone accounts registered on the device) to verify the identity of the user and to retrieve their health data records. • Requests access to location data (including background location) to retrieve local Covid-related information for the city where the user is located. • Requests access to the device camera to scan QR codes. • Requests access to the device storage to store files relating to the services and functionalities provided by the app.
	Third Party SDKs and Software Libraries: • *Google Mobile Services* – This library is used to provide location-based services in the app.
	Servers Contacted: • Microsoft (located in the United States) • Tehila (located in Israel)
Other Information	Tracking within the app is conducted using custom code on a Microsoft server hosted in the US.

SafeWA (Western Australia)	
Description	SafeWA is a contact tracing app launched by the Government of Western Australia that allows venue operators and citizens to easily register their attendance at relevant venues via a QR code. It is available for iOS and Android devices.
Developer(s)	Department of Health of the Government of Western Australia
Functionality	Contact tracing
Privacy Policy	Yes
Code Transparency	The app code is obfuscated and is not open source
Downloads (Google Play Store)	Over 500,000
Data Processed	Venue attended by user, time and date of scan, full name, and mobile number
Notable Data Access and Sharing	App Permissions: • Requests access to device camera to scan QR codes. • Requests permission to install packages (due to the inclusion of an external plugin called *open_file* developed by Crazecoder).[176]
	Third Party SDKs and Software Libraries: • *Google Firebase* – This SDK is used for tracking a range of activities within the app and monitoring app status. • *Sentry* – This is a tracking library that enables automatic reporting of errors, messages, and exceptions.
	Servers Contacted: • Government of Western Australia servers (located in Australia) • Amazon Web Services (located in the United States) • Google (located in the United States)
Other Information	The tracking information is recorded in the app (either by Google Firebase or Sentry) and transferred to servers located outside Western Australia.[177]

[176] See p.72 of the Tech Report.
[177] See p.75 of the Tech Report.

Scanner Voor CoronaCheck (Netherlands)	
Description	Scanner Voor CoronaCheck is the companion app for CoronaCheck used to scan QR certificates. It verifies the validity of a user's Covid-19 pass to check whether a user can access certain locations or participate in certain activities.
Developer(s)	Rijksoverheid
Functionality	Immunity passport
Privacy Policy	Yes
Code Transparency	The app code is not obfuscated and is open source
Downloads (Google Play Store)	Over 1 million
Data Processed	Full name, date of birth, IP address, and device metadata
Notable Data Access and Sharing	App Permissions: • Requests access to the device camera to scan QR codes.
	Third Party SDKs and Software Libraries: • *Google Mobile Services* – This software library is typically used for tracking purposes though this is not evident in the app.
	Servers Contacted: • Prolocation (located in the Netherlands)
Other Information	The app only contacts official government servers.