RECOMMENDATIONS ON PRIVACY AND DATA PROTECTION IN THE FIGHT AGAINST COVID-19

accessnow

Access Now defends and extends the digital rights of users at risk around the world. By combining direct technical support, comprehensive policy engagement, global advocacy, grassroots grantmaking, and convenings such as RightsCon, we fight for human rights in the digital age.

Recommendations on privacy and data protection in the fight against COVID-19

MARCH 2020

TABLE OF CONTENTS

I. EXECUTIVE SUMMARY

Access Now is committed to protecting human rights and to contributing to governments' responses to the coronavirus (COVID-19) outbreak. These responses must promote public health, prevent discrimination, ensure access to reliable and timely information, defend unrestricted access to an open, affordable, and secure internet, ensure the enjoyment of freedom of expression and of opinion, and protect privacy and personal data.

International and national laws recognize that extraordinary circumstances require extraordinary measures. This means that certain fundamental rights, including the rights to privacy and data protection, may be restricted to address the current health crisis as long as basic democratic principles and a series of safeguards are applied, and the interference is lawful, limited in time, and not arbitrary.

Governments, companies, NGOs, and individuals alike have a responsibility to do their part to mitigate the consequences of COVID-19 and to show solidarity and respect for each other. In this paper, we will provide **privacy and data protection recommendations for governments** to fight against COVID-19 in a rights-respecting manner.

There will be an aftermath to the COVID-19 outbreak. The measures governments put in place right now will determine this aftermath. The recommendations outlined below will ensure that the rule of law, and the rights to privacy and data protection, are protected throughout this crisis and in the future.

> *"We do always have to have in the back of our minds, especially when it comes to collecting information on individual citizens or tracking their whereabouts or movements, that there are always very serious data protection implications."* — Michael Ryan, Executive Director of the World Health Organisation's Health Emergencies Programme, 26 March 2020.[1]

This report is an Access Now publication. It is written by Estelle Massé. We would like to thank the Access Now team members who provided support, including Naman Aggarwal, Verónica Arroyo, Jennifer Brody, Sage Cheng, Fanny Hidvégi, Lucie Krahulcova, Peter Micek, Eric Null, Javier Pallero, Eliska Pirkova, Gaspar Pisanu, Dima Samaro, Raman Jit Singh Chima, Berhan Taye, and Donna Wentworth.

[1] World Health Organisation. *COVID-19 virtual press conference - 25 March 2020.* https://www.who.int/docs/default-source/coronaviruse/transcripts/who-audio-emergencies-coronavirus-press-conference-full-25mar2020.pdf

II. INTRODUCTION

Since late 2019, the world has been fighting the coronavirus disease (COVID-19). In response to what the World Health Organisation (WHO) has labeled a pandemic, governments around the world have been using technology to contain the spread of the virus and keep people safe. In spite of the time pressure, rights-infringing measures must be treated warily and be considered as extraordinary.

This paper will focus on three categories of measures that authorities have advanced around the world: (1) collection and use of health data, (2) tracking and geo-location, and (3) public-private partnerships. We will provide an overview of existing measures and give specific guidance for each category to help assist governments in addressing this major public health crisis while ensuring that people's rights are respected.[2]

POLICY-MAKING IN TIME OF CRISIS: What rules to respect when the exceptional becomes the norm?

In times of a global pandemic such as COVID-19, governments can assume special powers to introduce extraordinary measures to prevent and mitigate the health crisis, subject to international human rights law and additional domestic constitutional standards.[3]

What are the applicable norms?

Extraordinary powers and measures are strictly defined as specific forms of legal orders by national constitutions and legal regimes, and accepted in international and regional human rights law, including Article 4 of the International Covenant on Civil and Political Rights, Article 15 of the

[2] For more information on measures put in place around the world, please see: Privacy International. *Tracking the Global Response to COVID-19,* 2020.
https://privacyinternational.org/examples/tracking-global-response-covid-19

[3] United Nation Human Rights Office of the High Commissioner. *COVID-19: States should not abuse emergency measures to suppress human rights,* 2020.
https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=25722&LangID=E;
Michele Bachelet. *Coronavirus: Human rights need to be front and centre in response,* 2020.
https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx; and
Council of Europe. *We must respect human rights and stand united against the coronavirus pandemic*, 2020.
https://www.coe.int/en/web/commissioner/-/we-must-respect-human-rights-and-stand-united-against-the-coronavirus-pandemic.

European Convention on Human Rights and Article 27 of the American Convention on Human Rights.[4]

When and how can states use extraordinary powers?

These norms allow states the possibility of derogating, in exceptional circumstances and in a limited and supervised manner, from their obligations to guarantee certain rights and freedoms. The law defines the circumstances in which it is valid for a state to derogate from their obligations, limits the measures they may take in the course of any derogation, protects certain fundamental rights from any derogation, and finally sets out the procedural requirements that states must follow.

There are certain rights that do not allow for any derogation, such as the right to life, the prohibition of torture and inhuman or degrading treatment or punishment, the prohibition of slavery, and the rule of "no punishment without law."

How to apply extraordinary measures and what are the limits of these powers?

A special legal order such as a declaration of a state of emergency or danger is not an extra-legal situation; the rule of law continues to apply and there should be scope and time limitations.[5] Issuing a legal order does not make lawful every measure undertaken pursuant to it.

Special legal orders and measures should be written and broadcast, and disseminated broadly in appropriate languages and forums. They must have a sunset clause; indefinite term measures are not acceptable. Potential extension could be considered if necessary, but extraordinary measures must be limited in their severity, duration, and geographic scope. Governments and authorities must take every measure to restore regular rules as soon as possible at the end of a special legal order.

Fundamental human rights continue to apply in special legal orders or periods of emergency. Rights can only be restricted when necessary to prevent and mitigate the risks caused by the crisis, and restrictive measures must not go beyond the extent strictly required by and strictly proportionate to the exigencies of the circumstances.

[4] European Court of Human Rights. *Guide on Article 15 of the European Convention on Human Rights*, 2019. https://www.echr.coe.int/Documents/Guide_Art_15_ENG.pdf

[5] Hungarian Civil Liberties Union. *Unlimited power is not the panacea*, 2020. https://hclu.hu/en/articles/unlimited-power-is-not-the-panacea

III. COLLECTION AND USE OF HEALTH DATA

Health information is private and sensitive by nature and reveals intimate details of a person's life. The use, collection, and any other processing of this information should be protected, ideally through a comprehensive data protection law.[6] Use of health information — ranging from blood type, medical pre-conditions, gene information, temperature records, and more — is usually strictly limited. Nevertheless, during a public health crisis, the question is not *if* governments can use health data to help fight the crisis but *how* this can be done while safeguarding individual privacy and dignity to the maximum extent possible.

Protecting digital rights also promotes public health. According to the UN Committee on Economic, Social, and Cultural Rights, "The right to health is closely related to and dependent upon the realisation of other human rights, as contained in the International Bill of Rights, including the rights to food, housing, work, education, human dignity, life, non-discrimination, equality, the prohibition against torture, privacy, access to information, and the freedoms of association, assembly, and movement. These and other rights and freedoms address integral components of the right to health."[7]

In combating COVID-19, public authorities should be able to rely on data, including health data, to determine the best course of action to mitigate the spread of the virus and identify what measures must be taken to safeguard people and their rights during and after the crisis. Measures applied should be transparent, necessary and proportionate and, when they exist, data protection and privacy laws should have clear exceptions that apply to public health crises to allow for greater use of data than usual.

> *"During a public health crisis, the question is not if governments can use health data to help fight the crisis but how this can be done."*

[6] Access Now. *Creating a Data Protection Framework: a Do's and Don'ts Guide for Lawmakers,* 2018. https://www.accessnow.org/data-protection-handbook

[7] UN Committee on Economic, Social, and Cultural Rights. *The right to the highest attainable standard of health,* 2000. https://apps.who.int/disasters/repo/13849_files/o/UN_human_rights.htm

CASE STUDIES

In many countries, government authorities and private entities have publicised health data in an attempt to inform the public and provide individuals the opportunity to assess if they have been in contact with an infected individual. Unfortunately, because of the specificity of the data published — often without the name, but with several other unique identifiers — others have been able to track down infected individuals and their families. Publishing information related to health data during the COVID-19 crisis — including someone's positive or negative test results — not only raises challenges related to the protection of privacy and personal data, but it also creates threats to public order and security, risks discrimination, and even facilitates physical or online attacks and death threats.[8]

Below are regional case studies illustrating some of the uses of health data in relation to the fight with COVID-19 around the world. Based on these examples, we provide recommendations to governments on how to use data responsibly and in line with human rights law.

Latin America	In **Argentina**, a newspaper published personal information of people infected with COVID-19, indicating their age, where they had travelled, in which hospital they were treated, and more.[9] After this publication was noted and criticised by the public, they later made the names unavailable. The National Health Institute of **Perú** developed a platform where you can consult the health reports of patients who were tested for COVID-19 by entering their national identity document. For a few days, the information was therefore accessible to the public, not limited to the patient.[10] After receiving criticism, the national authorities included a second authenticator. To connect to the platform, an SMS-based code is now necessary.[11]

[8] The New York Times. *As Coronavirus Surveillance Escalates, Personal Privacy Plummets*, 2020. https://www.nytimes.com/2020/03/23/technology/coronavirus-surveillance-tracking-privacy.html
[9] La Nación. *Quiénes son y de dónde vinieron los 21 infectados por coronavirus en la Argentina*, 2020. https://www.lanacion.com.ar/sociedad/quienes-son-17-infectados-coronavirus-argentina-nid2341456
[10] Perú. *Instituto Nacional de Salud.* https://ins.gob.pe/resultado_coronavirus/
[11] Perú. *Debilidades de plataforma del Ministerio de Salud exponen información de pacientes COVID-19*, 2020. https://saludconlupa.com/noticias/peru-debilidades-de-plataforma-del-ministerio-de-salud-pueden-exponer-informacion-clinica-de-pacientes-covid-19/

Asia - Pacific	In **India**, at least two state governments — including the state of Karnataka, housing the tech hub of Bangalore — have uploaded PDF files online with names, house addresses, and travel history of people ordered into COVID-19 quarantines.[12] The information is accessible by everyone.
North America	**U.S.** citizen Frank King went on a cruise in Cambodia where he was mistakenly identified as a COVID-19 carrier. Even though Mr. King's test results were eventually corrected and all cruise-goers were determined to be healthy, upon returning to the U.S., he received death threats and personal attacks, online and off, for the following weeks.[13] Also in the **U.S**, more than 2,000 emergency medical workers at the University of California, San Francisco Medical Center and the Zuckerberg San Francisco General Hospital will take part in a study that involves wearing a smart ring in an attempt to identify people who have COVID-19 early. The rings will be given to emergency medical workers who come into contact with patients who may have COVID-19. The ring, which workers will have to wear for three months, collects health information such as peoples' heart rate, respiratory rate, and changes in body temperature. The device has not been proven to detect COVID-19.[14]

[12] Bangalore Mirror. *Government publishes details of 19,240 home-quarantined people to keep a check,* 2020. https://bangaloremirror.indiatimes.com/bangalore/others/government-publishes-details-of-19240-home-quarantined-people-to-keep-a-check/articleshow/74807807.cms

[13] The New York Times. *What It's Like to Come Home to the Stigma of Coronavirus,* 2020. https://www.nytimes.com/2020/03/04/us/stigma-coronavirus.html

[14] The Verge. *New study aims to use health data from a smart ring to identify coronavirus symptoms,* 2020. https://www.theverge.com/2020/3/23/21191225/coronavirus-smart-ring-oura-ucsf-san-francisco-general-hospital-tempredict

RECOMMENDATIONS

Apply data protection and privacy rights and principles

Governments and companies should apply the following data protection and privacy principles:

- ➔ **Purpose limitation and data minimisation**: Data collection, use, sharing, storage, and other processing of health data should be limited to what is strictly necessary for the fight against the virus. A pandemic is no excuse to collect extensive and unnecessary data.
- ➔ **Access limitation and data security**: Access to health data shall be limited to those who need information to conduct treatment, research, and otherwise address the crisis. The information should be stored securely, in a seperate database.
- ➔ **Data retention and future research**: Data processed in response to the crisis should be kept only for the duration of the crisis. Afterward, most health data shall be erased, though some non-identifiable information could be kept for historical and research purposes. This information should only be accessible and used for these public-interest purposes.
- ➔ **Do not sell health data:** Under no circumstance should health data be sold or transferred to third parties who are not working in the public interest.

Where public health crises occur and no matter whether countries have data protection and privacy laws in place, we should not abandon privacy and data rights. The core principles and users' rights should continue to apply.

Where data protection and privacy laws exist, they often have clear exceptions for public health crises, but they also provide a framework for safeguards around the increased ability to process data.

Finally, we encourage governments to follow guidance from independent data protection and privacy authorities. Authorities in México, Argentina, and the

	European Union, among others, have published guidelines for dealing with the use of health data in compliance with data protection laws.[15]
Do not disclose identifiable data about infected and cured patients publicly	Reporting of virus infections and statistics should not reveal personal information about patients. Specifically, identifiable information, especially name, date of birth, or address, about people affected by the virus should not be shared with the public. It endangers public order and places individuals at risk. Sharing this information privately should also be done with caution, as private entities may be seeking ways to monetise this data that go against privacy principles.
Involve experts and civil society	Where sensitive and personal information is collected, governments must involve experts from the privacy and health community to help develop and implement safeguards on the use of data, especially in countries that lack robust privacy or data protection authorities. Communities at risk of marginalization, including women and girls, those with disabilities, indigenous groups, the poor, LGBTQ persons, and religious and ethnic minorities, often suffer the brunt of discrimination and lack health care access, and should be consulted in creating specific, effective safeguards.
All crisis response measures should be transparent, necessary, and proportionate	A pandemic is not a time to reduce transparency. While transparency on its own is insufficient to protect individual privacy, people should still have the ability to understand what will happen with their data in a health crisis situation. Measures taken in response to pandemics should similarly be necessary and proportionate to ensure that responses will be beneficial to solving the crisis without sacrificing individual privacy.

[15] Infobae. *Coronavirus en México: el INAI emitió recomendaciones sobre el manejo de datos de los enfermos para garantizar su seguridad*, 2020. https://www.infobae.com/america/mexico/2020/03/14/coronavirus-en-mexico-el-inai-emitio-recomendaciones-sobre-el-manejo-de-datos-de-los-enfermos-para-garantizar-su-seguridad/ ; Agencia de Acceso a la Información Pública. *Tratamiento de datos personales ante el Coronavirus*, 2020. https://www.argentina.gob.ar/noticias/tratamiento-de-datos-personales-ante-el-coronavirus ; and European Data Protection Board. *Statement on the processing of personal data in the context of the COVID-19 outbreak*, 2020. https://edpb.europa.eu/our-work-tools/our-documents/other/statement-processing-personal-data-context-covid-19-outbreak_en

IV. TRACKING AND GEO-LOCATION

Location data is highly revealing. By simply following a person's movement based on location data from a smartphone, you can deduce their home address and workplace, map their interaction with others, identify their doctor visits, infer their socio-economic status, and more. Without proper safeguards, tracking and geo-location tools can enable ubiquitous surveillance.

In the context of a public health crisis, such as the COVID-19 outbreak, governments may want to rely on location tracking to map the evolution of the virus and plan responses. But such tracking comes with a number of concerns. First, it is important to note that tracking smartphone location will track *people's phones*, not the virus. Governments map the disease by cross-referencing peoples' location data with information on infected cases, a practice that has inherent risks. Second, even so-called anonymous location data can easily be re-identified; a study from 2013 showed that people could be reidentified from just four data points.[16] Third, geographic location might not be useful because people may drive, walk, take the subway, or work on the 50th floor of an 80 floor building; knowing a person's geographic location gives only part of the story, but still sacrifices personal privacy.[17] Finally, previous uses of phone records and location data in humanitarian response were shown to be inefficient and ineffective.[18] Thus, using geo-location to help address the spread of viruses should be conducted in a rights-respecting manner that promotes trust in government and protects individual safety and security, given the heightened risk of snowballing into state-sponsored mass surveillance.[19]

> *"Knowing a person's geographic location gives only part of the story, but still sacrifices personal privacy."*

[16] Wired. *Anonymized Phone Location Data Not So Anonymous, Researchers Find*, 2013. https://www.wired.com/2013/03/anonymous-phone-location-data/
[17] Lawfare. *Location Surveillance to Counter COVID-19: Efficacy Is What Matters*, 2020. https://www.lawfareblog.com/location-surveillance-counter-covid-19-efficacy-what-matters
[18] CIS-India. *Ebola: A big data disaster,* 2016. https://cis-india.org/papers/ebola-a-big-data-disaster
[19] European Data Protection Board. *Processing of personal data in the context of the COVID-19 outbreak*, 2020. https://edpb.europa.eu/news/news/2020/statement-edpb-chair-processing-personal-data-context-covid-19-outbreak_en

CASE STUDIES

In many countries, government authorities and private entities track people's movements to map "the spread of the virus" or to enforce lock-down and curfews. Often developed without appropriate safeguards, tracking measures expose private information that is not necessarily relevant for the fight against coronavirus and place a country's entire population under monitoring and surveillance.

Below are regional case studies that illustrate tracking and geo-location in response to the COVID-19 outbreak. Based on these examples, we provide recommendations to governments on how to use data responsibly and in line with human rights law.

Africa	In **Kenya**, the government is using "electronic surveillance" to track individuals who are supposed to self-isolate for 14 days due to their recent travel history. By mostly monitoring the mobile phone activities of travellers, including geo-location, sources have told *The Standard* that the government was able to identify individuals who defied the government order to self-isolate. Those in government-ordered self-isolation have also been told not to turn off their mobile phone and to always carry their devices.[20] In **South Africa**, telecom service providers, according to the Minister of Communications, Telecommunications and Postal Services, have agreed to share customers' location data with the government. It is not yet clear if it is only the location data of confirmed cases or that of the whole population that is being shared with the government. The minister has said that "the industry collectively has agreed to provide data analytics services in order to help [the] government achieve... [the fight against the virus]."[21]
Latin America	Through a state of emergency decree, the president of **Ecuador** established that satellite and mobile phone data can be used to monitor the location of people placed

[20] The Standard Media. *State Taps Phones of Isolated Cases,* 2020. https://www.standardmedia.co.ke/article/2001365401/state-taps-phones-of-isolated-cases
[21] Business Insider SA*. South Africa will be Tracking Cellphones to Fight the Covid-19 Virus. 2020,* https://www.businessinsider.co.za/south-africa-will-be-tracking-cellphones-to-fight-covid-19-2020-3

	under quarantine or mandatory isolation.[22] In a statement, civil society organisations asked the government for greater transparency and safeguards surrounding the decree.[23]
Asia - Pacific	In **South Korea**, the government has been tracking and posting online detailed location data of people confirmed and suspected to be infected by the virus.[24] By merging existing databases, new datasets provide dynamic tracking through CCTV footage, credit card histories, and location histories. The information published online includes a wealth of information, such as details about when people left for work, whether they wore masks in the subway, the name of the stations where they changed trains, the massage parlors and karaoke bars they frequented, and the names of the clinics where they were tested. As reported in *The New York Times*, internet mobs exploited this patient data to identify people by name and harass them.[25] **Taiwan** uses active mobile network monitoring to enforce home quarantine for newly arrived or at-risk individuals. Public authorities are alerted if an individual's mobile device is active outside of their home. This assumes that there is a documented link between each individual's identity, their phone number, and their residential address, which includes information on co-habitants.[26] To prevent those under home quarantine from circumventing the measures, public authorities call the number — reportedly twice a day — to ensure that the quarantined have not abandoned their mobile device and ventured outside.

[22] El Comercio. *Lenín Moreno decreta el estado de excepción en Ecuador por el covid-19*, 2020. https://www.elcomercio.com/actualidad/moreno-medidas-coronavirus-covid19-excepcion.html
[23] Asociación para el Progreso de las Comunicaciones. *Ecuador: Las tecnologías de vigilancia en contexto de pandemia no deben poner en riesgo los derechos humanos*, 2020. https://www.apc.org/es/pubs/ecuador-las-tecnologias-de-vigilancia-en-contexto-de-pandemia-no-deben-poner-en-riesgo-los
[24] The New York Times. *As Coronavirus Surveillance Escalates, Personal Privacy Plummets*, 2020. https://www.nytimes.com/2020/03/23/technology/coronavirus-surveillance-tracking-privacy.html
[25] The New York Times. *As Coronavirus Surveillance Escalates, Personal Privacy Plummets*, 2020. https://www.nytimes.com/2020/03/23/technology/coronavirus-surveillance-tracking-privacy.html
[26] Reuters. *Taiwan's new 'electronic fence' for quarantines leads wave of virus monitoring*, 2020. https://www.reuters.com/article/us-health-coronavirus-taiwan-surveillanc-idUSKBN2170SK

Europe	All over the **European Union**, telecom companies and public authorities are entering into arrangements to share location data. So far, there is little transparency as to how much data is being shared, and how long these arrangements, which are often extra-legal, will last. It is also unclear whether companies are providing records of metadata or allowing governments to conduct real-time monitoring of people: ➔ In **Belgium**, telecommunications companies including Orange and Proximus agreed to share "parts of their database" to help authorities tackle the coronavirus outbreak.[27] ➔ In **Germany**, Deutsche Telekom is giving part of its location data to the Federal Disease Prevention Agency to help contain the pandemic. In addition to national governments, the European Commission requested aggregated metadata from telecoms operators to "track the spread of the virus" and determine where the need for medical supplies is the most pressing.[28] At the moment, this request is not based on legal requirements and therefore cannot be scrutinised.
North America	In the **United States**, researchers are using Facebook data to measure social distancing.[29] Data collected from Facebook users who have location history enabled is used to develop maps with aggregated, de-identified location data. This project presents significant privacy and data protection risks since it assumes that Facebook users agree to be tracked by the platform in the fight against coronavirus.

[27] Le Soir. *Coronavirus: le cabinet De Block dit «oui» à l'utilisation des données télécoms*, 2020. https://plus.lesoir.be/286535/article/2020-03-12/coronavirus-le-cabinet-de-block-dit-oui-lutilisation-des-donnees-telecoms
[28] Politico. *Commission tells carriers to hand over mobile data in coronavirus fight,* 2020. https://www.politico.eu/article/european-commission-mobile-phone-data-thierry-breton-coronavirus-covid19/
[29] Protocol. *Facebook data can help measure social distancing in California*, 2020. https://www.protocol.com/facebook-data-help-california-coronavirus

RECOMMENDATIONS	
Consider all possible options to map the spread of the virus	A few countries decided against the use of geo-location or tracking, and instead opted for detailed in-person contact tracing. This method, in addition to testing at scale to identify infected people, presents fewer opportunities to undermine the right to privacy while allowing for the accurate mapping of the virus.
Consider that location data may be flawed	The use of location data to determine whether people have been in contact with someone infected by the virus has significant limitations. Cell tower location tracking lacks granularity. It can track general phone locations, meaning it can place phones in their general vicinity, but it cannot detect whether two phones were within two meters, which would be required for relevant data in the case of COVID-19. GPS signals could offer finer precision but do not work inside buildings or transports, and there can be interference from tall buildings, which means that large parts of a city might not be covered.[30] Again, knowing a person's geographic location gives only part of the story, yet sacrifices personal privacy, and governments should not rely on geo-location tracking. It may be that close-range Bluetooth polling between phones could determine how many people have been in close contact, but there remain privacy implications with this technique and its use should only be explored if it is done transparently with safeguards on access, retention, and use.
Protect the rule of law: data-sharing agreements between states and companies must be based in law	When governments and public authorities determine that data-sharing agreements are necessary for the fight against the virus, they must rely on existing or emergency laws. The inherent privacy and data protection risks of these measures mean that public and independent authorities must be able to scrutinise the measures, which should also be limited in time. Therefore, governments should ensure its agreements follow legal norms and are transparent. Ad-hoc, extra-legal, and opaque deals with telecoms operators and companies to share location data are not acceptable.

[30] Lawfare. *Location Surveillance to Counter COVID-19: Efficacy Is What Matters*, 2020. https://www.lawfareblog.com/location-surveillance-counter-covid-19-efficacy-what-matters

Use anonymised data and apply data protection and privacy principles	When governments decide to use location data under existing or emergency laws, we recommend that they rely on anonymised data. Importantly, even so-called anonymous data can easily be re-identified, and even just four data points can be sufficient, which means that data protection and privacy risks remain.[31] Data protection and privacy principles must therefore apply, including data minimisation to ensure that the data used are relevant, accurate, and necessary to address the current crisis, and use limitations to ensure data are used only for crisis response. Furthermore, telecoms operators and companies providing data should work with supervisory authorities and privacy experts to ensure data are used with appropriate safeguards. Finally, we urge governments to limit access to this data to those that require the information to fight the virus. The data should either be tagged, or stored in a separate database for crisis response, in such a way that it can be easily deleted when the crisis is over.
Learn from past mistakes: do not deploy mass surveillance	A pandemic should not serve as an excuse for the deployment of new, general surveillance powers. In responding to past health crises, we have learned that deploying invasive surveillance is misguided and potentially harmful, for both human rights and public health. Indeed, the deployment of big data tracking during the ebola outbreak led to the violation of millions of people's right to privacy, while doing very little to combat the disease.[32] In relation to tracking, governments should not require citizens to enroll in tracking applications or services as it would result in new forms of surveillance.
Do not establish disproportionate data retention mandates	The current health crisis should not be used as an opportunity to establish disproportionate data retention mandates. The necessary information to fight the virus must be up-to-date and, therefore, does not need to be maintained for many years. Generally, data should be deleted as soon as the crisis is over.

[31] Wired. *Anonymized Phone Location Data Not So Anonymous, Researchers Find*, 2013. https://www.wired.com/2013/03/anonymous-phone-location-data/
[32] The Centre for Internet & Society. *Ebola: A Big Data Disaster*, 2016. https://cis-india.org/papers/ebola-a-big-data-disaster

V. PUBLIC-PRIVATE PARTNERSHIPS: APPS, WEBSITES, AND SERVICES USED AS A RESPONSE TO COVID19

Since the beginning of the crisis, governments and tech companies have been working together to develop technological solutions to fight the COVID-19 outbreak. From gathering data, tracking infected citizens' movements, disseminating public health alerts, to monitoring the general public's whereabouts, the private sector is offering a plethora of techno-solutions to public authorities. In any public crisis, solidarity among all actors of society is necessary.

In particular, the ongoing crisis highlights how much the public and public authorities are depending on tech companies to function: from providing broadband access, to allowing people to work from home, to providing video-conferencing solutions or tools that respond directly to the crisis, such as diagnosis apps. But without appropriate safeguards and meaningful human rights considerations, technological solutions come with many risks. By relying on private companies, governments may enhance the powers of dominant platforms, exacerbate the risks associated with data harvesting and monetisation of health information, and legitimise privacy-invasive services. What is more, a number of companies known for enabling human rights violations are publicly offering products to respond to COVID-19 that could be repurposed for mass surveillance once the crisis ends.[33]

> *"By relying on private companies, governments may enhance the powers of dominant platforms, exacerbate the risks associated with data harvesting and monetisation of health information, and legitimise privacy-invasive services."*

CASE STUDIES

A large number of apps, websites, and other online services have emerged to help people map, combat the spread of COVID-19, cope, and organise during the outbreak. The tech

[33] See for instance: Ranking Digital Rights. *Corporate Accountability Index*, 2019. https://rankingdigitalrights.org/index2019/; The Wall Street Journal. *To Track Virus, Governments Weigh Surveillance Tools That Push Privacy Limits,* 2020. https://www.wsj.com/articles/to-track-virus-governments-weigh-surveillance-tools-that-push-privacy-limits-11584479841 ; and Bloomberg. *Israeli Spyware Firm Wants to Track Data to Stop Coronavirus Spreading,* 2020. https://www.bloomberg.com/news/articles/2020-03-17/surveillance-company-nso-supplying-data-analysis-to-stop-virus

sector has an important role to play in contributing to the public response to this crisis. However, the long-standing mediocre human rights track record of most tech companies, in particular in the area of privacy and data protection, is a significant challenge in finding sustainable solutions to fight the outbreak.

Below are regional case studies that illustrate some of the tech companies' proposals to combat COVID-19. Drawing from these examples, we provide recommendations to governments on how to use data responsibly and in line with human rights law.

Africa	In **Kenya**, *mSafari* app is being rolled out to help with contact tracing.[34] The app currently being developed by the private sector will reportedly be used to track passengers in public service vehicles including buses, taxis, and other transportation services. Drivers are expected to download this app and register all passengers. At the time of publication, the website of *mSafari* did not have terms or any policies available publicly that explain what information is being collected, with whom the information may be shared, or how it will be processed.[35]
Latin America	In **Argentina**, the President and government representatives held a videoconference with tech companies asking them to develop an app to help stop people from leaving their houses.[36] In **Colombia**, an old app was repurposed and renamed CoronApp to provide information on the virus.[37] The application requests a large amount of personal information — such as data on ethnicity — to function. There is no transparency regarding who has access to this data and how it may be used. In **Guatemala**, the government has launched an official application to inform people about COVID-19 called Alerta Guate. To download the app, users have to allow access

[34] The Standard. *Government to Launch Contract Tracking Application,* 2020. https://www.standardmedia.co.ke/health/article/2001365263/app-uses-passenger-data-to-trace-virus-path
[35] *mSafari,* 2020. http://msafari.co.ke/
[36] Gobierno Nacional de Argentina. *Soluciones conjuntas entre el Gobierno y empresas tech para enfrentar el Coronavirus*, 2020. https://www.argentina.gob.ar/noticias/soluciones-conjuntas-entre-el-gobierno-y-empresas-tech-para-enfrentar-el-coronavirus
[37] Fundación Karisma. *CoronApp, una barrera para el acceso a información pública y una pesadilla para la privacidad*, 2020. https://stats.karisma.org.co/coronapp-inscolombia/

	to location data, phone microphone, and provide an email address or phone number.[38]
Middle East and North Africa	In **Tunisia**, Enova Robotics signed an agreement with the Ministry of Interior to start operating PGuard robots.[39] These robots will be equipped with a set of infrared cameras and used to stop people from leaving their houses. There is no information as to where these robots will be deployed, what information they will gather, how long they will keep the data and who would have access to it. The infamous NSO Group is exploiting the global crisis by pitching its tracking services to governments around the world.[40] The company's hacking software has been implicated in countless human rights violations, perhaps most notably the murder of Jamal Khashoggi.[41] The application currently being developed by the NSO Group, and alleged to be tested in about a dozen countries, takes two weeks of mobile-phone tracking information from an infected person, then matches this information with location data collected by national mobile phone companies.[42] The app aims to pinpoint people who were in the patient's vicinity for more than 15 minutes, and could therefore be vulnerable to contagion.

[38] La Hora. *Sandoval sobre Alerta Guate: "Quien la quiera descargar lo puede hacer"*, 2020. https://lahora.gt/sandoval-sobre-alerta-guate-quien-la-quiera-descargar-lo-puede-hacer/
[39] African Manager. *A first in Tunisia: Pguard, the security robot to report violations*, 2020. https://africanmanager.com/une-premiere-en-tunisie-pguard-le-robot-de-securite-pour-signaler-les-infractions/
[40] Bloomberg. *Israeli Spyware Firm Wants to Track Data to Stop Coronavirus Spreading*, 2020. https://www.bloomberg.com/news/articles/2020-03-17/surveillance-company-nso-supplying-data-analysis-to-stop-virus
[41] The New York Times. *Israeli Software Helped Saudis Spy on Khashoggi, Lawsuit Says*, 2020. https://www.nytimes.com/2018/12/02/world/middleeast/saudi-khashoggi-spyware-israel.html
[42] Independent. *Coronavirus: Controversial Israeli spyware firm NSO builds software tracking mobile data to map Covid-19*, 2020. https://www.independent.co.uk/news/world/middle-east/coronavirus-israel-cases-tracking-mobile-phone-nso-spyware-covid-19-a9410011.html

Asia - Pacific	In **China**, apps such as Alipay and WeChat flagged high-risk individuals, who were then quarantined or disallowed from entering public spaces. As normalcy returns to the region, people are required to obtain a "green clearance" from these apps to be allowed back into public life and move freely.[43] Also in **China**, companies like SenseTime claim that their contactless temperature detection software has been deployed in Beijing, Shanghai, and Shenzhen. The company also claims to have a facial recognition tool. While facial recognition cameras are commonplace in China, these cameras are being upgraded for greater accuracy and temperature detection.[44] **Singapore** has an app called Tracetogether. It allows people to voluntarily share their information, and tracks other people with whom they come in contact via bluetooth. If any of the app's users contract COVID-19, all users who have come in contact with said person are notified, along with the government. There is also no transparency as to who may have access to this information.
Europe	In **Spain**, both the region of Madrid and the Catalonian government have built apps to inform the population about COVID-19 symptoms.[45] The applications collect health and real-time location data from the population to create heat maps. **Slovakia** has an app called Zostan Zdravy ("stay healthy"). It aims to inform the user if someone infected with COVID-19 is in close proximity.[46] So far, the app has been downloaded over 10,000 times and works as follows: 1. user downloads the app for "free"; 2. user registers with their phone number or email;

[43] The New York Times. *In Coronavirus Fight, China Gives Citizens a Color Code, With Red Flags,* 2020. https://www.nytimes.com/2020/03/01/business/china-coronavirus-surveillance.html
[44] BBC. *Coronavirus: China's tech fights back*, 2020. https://www.bbc.com/news/technology-51717164
[45] Carto. *CARTO collaborates on 'AsistenciaCovid19' App against Coronavirus*, 2020. https://carto.com/blog/carto-develops-app-against-coronavirus/ and CatalanNews. *How the health department's new app to monitor coronavirus symptoms works,* 2020. https://www.catalannews.com/society-science/item/how-the-health-department-s-new-app-to-monitor-coronavirus-symptoms-works
[46] TechBox. *Appka Zostaň zdravý upozorní na koronavírus v okolí*, 2020. https://techbox.dennikn.sk/aplikacia-zostan-zdravy-vas-upozorni-na-potvrdenie-koronavirusu-vo-vasom-okoli/

3. the app generates a database of potential close exposure to people infected with COVID-19. The user is not provided with information about how the database was created;
4. user can purportedly see whether, when, and how close they have been to someone infected with confirmed COVID-19;
5. anonymous devices that were in close proximity of identified infection will receive information about their possible exposure to COVID-19 and will be asked to take the test;
6. user can request to be tested for COVID-19 via the app using an "anonymous identification" code;
7. user will go to the hospital for a test. If a user tests positive, medical staff members will be given the user's identification code and will insert it into the health system. The user will then obtain test results through the app. The system then sends out a warning message to all other users of the app who were in close proximity of said person who tested positive.

In **Poland**, the government launched an app to monitor quarantined patients. Patients are required to take selfies to prove they are quarantining properly. The alternative is to receive unexpected visits from the police. Upon registering with a selfie, residents of Poland must comply with periodic requests for geo-located selfies.[47] Except for the registration selfie, the data uploaded to and stored by the app will be deleted when the individual's quarantine ends. The registration selfie will be stored for six years.[48]

[47] Business Insider. *Poland made an app that forces coronavirus patients to take regular selfies to prove they're indoors or face a police visit*, 2020. https://www.businessinsider.com/poland-app-coronavirus-patients-mandaotory-selfie-2020-3?r=US&IR=T

[48] Niebezpiecznik. *Aplikacja "kwarantanna domowa" wzbudza obawy o inwigilację. Czy słusznie?*, 2020. https://niebezpiecznik.pl/post/aplikacja-kwarantanna-domowa-wzbudza-obawy-o-inwigilacje-czy-slusznie/

North America	In the **United States**, developers are working on an app that would let people log their movements and compare them with those of known COVID-19 patients, using data supplied by the state or national public health departments. Over time, users would be asked whether they are infected. It is unclear who would have access to this information.[49] Also in the **U.S.**, Alphabet's Verily launched a limited COVID-19 screening website.[50] To qualify for screening, it requires users to have a Google account and agree to information being potentially shared with Google.[51] The website is a collaboration between the Bay Area-based biotechnology company, the California governor's office, and other local, state, and federal officials.

[49] Wired. *Phones Could Track the Spread of Covid-19. Is It a Good Idea?,* 2020. https://www.wired.com/story/phones-track-spread-covid19-good-idea/

[50] CNBC. *Alphabet's Verily launches a limited coronavirus screening website*, 2020. https://www.cnbc.com/2020/03/15/alphabets-verily-says-it-will-launch-a-limited-coronavirus-testing-website-monday.html

[51] Project Baseline by Verily. *California COVID-19 risk screening and testing*. https://www.projectbaseline.com/study/covid-19/

RECOMMENDATIONS	
Bring transparency to public-private partnerships	Collaborations between governments, authorities, and companies or other organisations must be transparent. They should follow open data, open government, open procurement standards, and transparency reporting requirements, and facilitate the public's access to information. To encourage competition, software or services should not be conditioned on long-term or exclusive contracts. Governments need flexibility to choose the best partners in the public interest.
Conduct mandatory human rights impact assessments and due diligence processes for every public-private partnership and public procurement	**For private-sector actors:** Private-sector actors that design, develop, or implement systems to tackle COVID-19 should follow an industry standard human rights due diligence framework to identify salient risks, avoid fostering or entrenching discrimination, and respect human rights more broadly through all lifecycles of their systems. As necessary, private sector actors should create processes to monitor, mitigate, and report on potential harms and notify affected individuals. **For the public sector:** Mandatory human rights impact assessments should: ➔ Be conducted regularly, prior to public procurement, during development, at regular milestones, and throughout their context-specific use,[52] ➔ Include an evaluation of the possible transformations that they may bring upon existing social, institutional, or governance structures, and ➔ Be made available to the public in an easily accessible and machine-readable format. Where it is not possible to meaningfully mitigate the identified risks, the system should not be deployed or otherwise used by any public authority. These assessments shall be expedited to be able to respond to the crisis.

[52] Danish Institute for Human Rights. *Driving change through public procurement*, 2020. https://www.humanrights.dk/publications/driving-change-through-public-procurement

Consider the human rights track record of companies and exclude actors that systematically violate human rights	Governments should consider the additional risks of outsourcing state activities in their COVID-19 response to the private sector before they enter into public-private partnerships. Governments must ensure that private entities' solutions are proven and provide demonstrable benefits before collaborating. Governments should ensure their partners comply with human rights safeguards. Companies with a track record of violating or facilitating violations of human rights should be excluded from participating in public calls to provide technical solutions and applications to address the pandemic.[53]
Apply privacy and data protection principles	Companies developing apps and services used to cope with or respond to the COVID-19 outbreak must provide users with data protection rights, and abide by the principles of data minimisation, purpose and use limitation, and limited access and data retention.[54]
Prohibit private companies from re-using or monetising data	When creating applications to respond to a public health crisis, private companies should not be able to monetise data derived from the use of their products. Additionally, there should be clear limitations on secondary uses or further processing of data.

[53] Companies that have built their business model around undermining the security and integrity of our digital infrastructure cannot be trusted to build a non-intrusive application in the service of public health. See Ranking Digital Rights. See: *Corporate Accountability Index*, 2019. https://rankingdigitalrights.org/index2019/; The Wall Street Journal. *To Track Virus, Governments Weigh Surveillance Tools That Push Privacy Limits,* 2020. https://www.wsj.com/articles/to-track-virus-governments-weigh-surveillance-tools-that-push-privacy-limits-11584479841 ; and Bloomberg. *Israeli Spyware Firm Wants to Track Data to Stop Coronavirus Spreading,* 2020. https://www.bloomberg.com/news/articles/2020-03-17/surveillance-company-nso-supplying-data-analysis-to-stop-virus

[54] See our recommendation "Apply data protection and privacy rights and principles," in section III of this paper. For more information, see also: Access Now. *Creating a Data Protection Framework: a Do's and Don'ts Guide for Lawmakers,* 2018. https://www.accessnow.org/data-protection-handbook

Allow for the open and transparent review of products	Any private-sector application or technological solution to help fight COVID-19 should be open to full scrutiny and audits by both independent regulatory authorities and civil society groups.
Push back against "techno-solutionism"	We must remain vigilant toward technological solutions proposed in a high-risk scenario such as health crises, with particular scrutiny for artificial intelligence and facial recognition projects. Tried and tested measures should be preferred to novel technological quick fixes, especially when the latter involves transgressing legal protections and harvesting personal data.
Do not invest in controversial surveillance systems	While resources for public health are scarce, governments around the world should not see this health crisis as an opportunity to invest in controversial surveillance systems, such as facial recognition technology.

VI. CONCLUSION

The world is facing a significant public health crisis; responses and measures adopted by governments to fight COVID-19 will have an impact beyond this emergency. From past health crises, we have learned not to fall for quick fixes, but to uphold human rights to prevent further harms for the population. Data and technology will be key components in the fight against COVID-19. The question is not *if* governments can use data and tech to help fight the virus but *how*; here our message is simple: **protecting digital rights also promotes public health**.

In a time of crisis, public trust is key to ensure that everyone unites behind the response. Eroding human rights would be misguided and harmful, both during and in the aftermath of the crisis. In this collaborative fight against COVID-19, we all have a responsibility to act, advise, and protect: governments, companies, NGOs, and individuals. We hope that the recommendations we present to governments will contribute to finding a common response to this crisis, and we stand ready to further advise on its implementation.

> *"Asking people to choose between privacy and health is, in fact, the very root of the problem. Because this is a false choice. We can and should enjoy both privacy and health. We can choose to protect our health and stop the coronavirus epidemic not by instituting totalitarian surveillance regimes, but rather by empowering citizens."* — Yuval Noah Harari [55]

For more information, please contact:
Estelle Massé
Senior Policy Analyst and Global Data Protection Lead, Access Now
estelle@accessnow.org

[55] Financial Times. *The world after coronavirus*, 2020. https://www.ft.com/content/19d90308-6858-11ea-a3c9-1fe6fedcca75