Guidance to UNDP Country Offices on the privacy, data protection and broader human rights dimensions of using digital technologies to combat Covid-19

1. Digital response to Covid-19

Covid-19 has generated a global rush to find tools and resources to guide and enable government responses. The most urgent need has been for data, including personal data, and readily available instruments to enable authorities to quickly detect cases and trace contacts in order to control the spread of the virus, as well as manage the information flow to ensure an orderly and strategic response. This has led to a patchwork of measures developed at speed (some by governments, others by private sector entities that offer them to governments[1]), with many of them leaning on the power of digital technologies (particularly mobile devices) to enable expeditious, comprehensive, real-time data grab and analysis. Some of the approaches employed by governments (in cooperation with the private sector) that have received the most media coverage are digital tracking and surveillance tools that employ various forms of 'contact tracing' of either people that have tested positive for Covid-19, or their 'at risk' contacts, as well as quarantine/self-isolation enforcement mechanisms.[2]

While many digital solutions have proved successful in slowing down or isolating the spread of the virus, these tools may present profound challenges to privacy rights. The challenges require inspection, particularly as many of these efforts are being deployed in different country contexts, with different levels of privacy and rights frameworks, and where governments are functioning in non-normal capacities and making decisions under "rules of exception" (e.g., extra-ordinary powers that may be triggered by national emergencies such as a pandemic, and which may pose risks to individual rights and civil liberties). UNDP County Offices (COs) across the world have quickly responded to requests for support from Member States to assist in containing the spread of Covid-19. This Guidance Note advises COs on some of the privacy and data protection rights, freedom of information and other human rights dimensions of digital responses to Covid-19 that can inform the response of COs to requests from national counterparts.

2. UN and UNDP privacy and data protection policy

The International Covenant on Civil and Political Rights provides that "no one shall be subjected to arbitrary or unlawful interference with his or her privacy"[3] and that "everyone has the right to the protection of the law against such interference or attacks."[4] In recent years, there have been a number of reports from the UN High Commissioner for Human Rights and various UN Special Rapporteurs to the

[1] Apple and Google, for example, have announced an API interface intended to work with apps run by government public health ministries (as in Singapore), arguing that, without a public-health-competent human in the loop, there are other risks like fake 'false positives' which can spread alarm.
[2] See Annex I for a list of some of the more widely known measures.
[3] Article 17.1.
[4] Article 17.2.

UN Human Rights Council that focus either directly or indirectly on privacy and data protection.[5] There have also been a number of UN Resolutions on the topic: two of the General Assembly,[6] two of the Human Rights Council,[7] as well as a Security Council Resolution on counter-terrorism that specifically includes discussion on biometric technology.[8] While these reports and resolutions (as well as the SG's February 2020 call to action on human rights)[9] stress the importance of privacy and protection of personal data, and the need for Member States to consider the impact of the embrace of digital technologies on these principles and rights, there is no UN instrument that specifically advises Member States on *how* they should specifically protect personal data in the maximum way possible to protect privacy, with a sanctions mechanism to enforce implementation of same, in the same way that the European Union 2018 General Data Protection Regulation does ("widely considered to be the baseline privacy standard of today").[10]

The individual UN agencies, funds and programmes that directly handle and process Personally-Identifying Information (PII) of their client population, such as UNHCR, WFP and IOM,[11] have developed detailed data protection policies that govern their handling of such data.[12] As UNDP rarely handles PII,[13] it has not developed either any specific data policy on handling of personal data, or any specific legal or policy guidance to Member States, to date, on development of either privacy or data protection legislative frameworks. UNDP has, however, contributed to the development of the UN Sustainable Development Group's "Data Privacy, Ethics and Protection: Guidance Note on Big Data for Achievement of the 2030 Agenda," drafted for the former UNDG by UN Global Pulse in 2017.[14] Some Country Offices[15]

[5] A/HRC/39/29, "*The Right to Privacy in the Digital Age – Report of the High Commissioner for Human Rights*," August 2018; A/HRC/23/40, "*Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*," December 2013, A/HRC/43/52, "*Report of the Special Rapporteur on the right to privacy*," and; A/74/493, *"Extreme poverty and human rights,"* October 2019.

[6] A/RES/45/95, "*Guidelines for the Regulation of Computerized Personal Data Files*," December 1990, A/RES/68/167, "*The Right to Privacy in the Digital Age*," December 2013.

[7] HRC/RES/41/11, "New and emerging digital technologies and human rights," July 2019, and; HRC/RES/42/15, "The right to privacy in the digital age," September 2019.

[8] SCR 2396 of 2017 (S/RES/2396), "decides that Member States shall develop and implement systems to collect biometric data, which could include fingerprints, photographs, facial recognition, and other relevant identifying biometric data, in order to responsibly and properly identify terrorists, including foreign terrorist fighters, in compliance with domestic law and international human rights law, (and) calls upon other Member States, international, regional, and sub-regional entities to provide technical assistance, resources, and capacity building to Member States in order to implement such systems, and encourages Member States to share this data responsibly among relevant Member States, as appropriate" The lack of privacy protections in SCR2396, beyond 'responsibly sharing,' has drawn adverse comment from the UN Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism. To assist Member States implement SCR2396, the UN Counter Terrorism Executive Directorate launched, in 2018, a "*Compendium of recommended practices for the responsible use and sharing of biometrics in counter-terrorism*," https://www.un.org/sc/ctc/wp-content/uploads/2018/06/Compendium-biometrics-final-version-LATEST_18_JUNE_2018_optimized.pdf https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=25603&LangID=E

[10] "*Africa's Rising Leadership in Privacy*," Pam Dixon, Executive Director, World Privacy Forum, published at www.id4africa.com

[11] These agencies *directly register* their client population for the services they provide, whereas both UNDP (for mass voter or national identity registration) and UNICEF (for birth registration) assist national government counterparts in *their* registration of their respective client populations.

[12] For example, "*Policy on the Protection of Personal Data of Persons of Concern to UNHCR*," UNHCR, May 2015.

[13] Moving forward, UNDP will need to handle PII, including through its reintegration programmes or in partnerships such as with UNU.

[14] https://unsdg.un.org/resources/data-privacy-ethics-and-protection-guidance-note-big-data-achievement-2030-agenda

[15] E.g., Indonesia and the Philippines

have adopted the UN Global Pulse principles and standards when developing apps to support government partners.[16]

Since the onset of Covid-19, the Office of the UN High Commissioner for Human Rights has issued guidance on the human rights dimensions of Covid-19 including on privacy,[17] as have other UN entities for their constituencies.[18]

Annex II includes links to a suite of tools and principles, including the UN Pulse's Due Diligence Questionnaire and Checklist (which could be applied before engagement with technology partners), the Risks, Harms and Benefit Assessment tool, UNDG's Principles on Data Privacy and Protection, and the UNSCEB Principles on Personal Data Protection and Privacy.

3. Key privacy and data protection challenges in the Covid-19 digital response

Lack of opportunity for public deliberation during crisis

According to international and national laws, during states of emergency, certain rights and freedoms can be suspended or restricted, including the right to privacy and data protection.[19] Due to the need for immediate action on Covid-19, some governments quickly took strong measures that pose risks to individual privacy, reputation and security.

Moreover, given the backdrop of a health crisis, some of these measures were launched absent or with little opportunity for public discussion with parliament, civil society (particularly those focused on privacy) and the general public, leading some to call urgently for transparency measures.[20] General advice (offered via the UN Resident Coordinator, where appropriate) should be given that emergency powers be lifted as soon as possible and constitutional power be restored to parliaments, other legislative bodies and the judiciary, once the emergency has subsided.[21]

[16] As co-chair of the UN Legal Identity Agenda Task Force (along with UNICEF and UNDESA), UNDP will be working with OHCHR, UNHCR and others in the development of further policy guidance for Member States on privacy and protection of personal data in the context of national identity schemes in 2020-2021.

[17] https://www.ohchr.org/EN/NewsEvents/Pages/COVID19Guidance.aspx

[18] For example, UNICEF: https://www.unicef.org/globalinsight/stories/covid-19-and-childrens-digital-privacy

[19] Article 4 of the International Covenant on Civil and Political Rights, for example, provides for derogation from obligations in times of public emergency "to the extent strictly required by the exigencies of the situation, provided that such measures are not inconsistent with their other obligations under international law and do not involve discrimination solely on the ground of race, colour, sex, language, religion or social origin." When a State party does avail itself of the right of derogation, it is to immediately inform the other State parties through the UNSG and communicate the date it terminates such derogation. (https://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx).

[20] https://www.accessnow.org/cms/assets/uploads/2020/03/Access-Now-recommendations-on-Covid-and-data-protection-and-privacy.pdf

[21] The European Union, in its advice to governments, states that measures need to be justified, proportionate and temporary, remain strictly limited to what is necessary to combat the crisis, and should end "without adequate justification" after the emergency has passed. (https://ec.europa.eu/info/sites/info/files/recommendation_on_apps_for_contact_tracing_4.pdf).

Lack of general privacy and data protection regulations

Many countries do not have strong privacy and data protection legislative and institutional frameworks or adequate public oversight and control. Combined with the fact that it is often the private sector that has created or facilitated the use of technology for Covid-19 response, privacy and data protection rights are being put at risk in the absence of adequate guidance on the legal and ethical norms for collecting, processing, using and storing personal data.

4. Covid-19-specific digital guidance for UNDP Country Offices

General Principles

All citizens have rights to be informed on usages of their data for Covid-19 response by government and private sector while developing/implementing technologies. UNDP, based on two resolutions of the Human Rights Council referenced earlier, can advise governments to understand the privacy issues on their Covid-19 responses and support governments in engaging with the private sectors while bearing in mind the data/privacy issues.

1. Human-rights-based approach

In response to Covid-19, we should be guided by the human-rights-based approach. In the SG's call to action for human rights[22] launched on 24 February, one of the seven areas concerns new frontiers of human rights – which include digital technologies.

2. Participatory approach

In line with the SG's call for digital cooperation,[23] where possible, UNDP advises to involve diverse actors (governments, civil society organizations, academia, the private sector) and make sure that all stakeholders participate and positively contribute their expertise to the new technologies on promoting and protecting human rights.

3. Consent

People have the right to be informed of the data collected from them and how the data will be used, stored and managed, including information about who has access to the data. Consent needs to be secured from data subjects and the extent of their participation should be clear. 'Opt-in' options for apps, for instance, need to be clear that participation in the effort is voluntary and that the user has the

[22] https://www.un.org/sg/sites/www.un.org.sg/files/atoms/files/The_Highest_Asperation_A_Call_To_Action_For_Human_Right_English.pdf. Particularly relevant in this case are: 1. Support Member States to ensure that human rights principles inform implementation of the 2030 Agenda, including empowering people and creating avenues for civil society participation, as well as taking human-rights-sensitive, non-discriminatory approaches to data collection, monitoring and reporting. This is the surest way to bring the benefits of the ambitious and far-reaching agenda to all, leaving no one behind. 2. Promote effective data protection and the right to privacy, particularly where personal and health-related data are concerned.

[23] https://www.un.org/en/digital-cooperation-panel/

power to cease participation at any time and that all data about the user will be deleted permanently upon exit.

4. Anonymization/pseudonymization of personal data

All efforts, either legislative, regulatory or as a matter of operational procedure, should be made to ensure that the identity (or clues to the identity) of persons that have tested positive for Covid-19 are concealed from the media and the public. To minimize the risk of a data breach, only health officials should decide which data can be anonymized (scrubbed for any information that may serve to identify the data subject) and which can be pseudonymised (does not remove all identifying information from the data but reduces the linkability of the data with the original identity, e.g., via encryption).[24]

5. Temporary nature of digital 'tracking' and surveillance measures

Measures taken by national governments to digital tracking of individuals, groups of individuals or entire communities should not be discriminatory or inconsistent with their other obligations under international law. They should be strictly temporary and should be terminated once public emergency threat of Covid-19 has subsided for that jurisdiction.

6. Collection, use and duration of storage of data

There should be strict guidelines outlining the purposes for which data may be used (which should be specifically limited to public health), where data reside and are stored and who has access to them. The purpose needs to be specifically related to and used for public-health-specific aims and should be limited in scope and duration as required in the particular situation. These guidelines should be made available to the public/all persons whose data is collected. Adequate measures should be in place to ensure that these guidelines are observed and to prevent unauthorized access to or storage of data. This is particularly relevant given the collection of blood plasma from recovered Covid-19 patients. Safeguards should protect against misuse of data by governments or companies to avoid the collection or use of confidential private information for purposes not related to the public health crisis.

7. Gender dimensions of digital response

Digital technologies are not gender-neutral in their accessibility and impact. The UN Special Rapporteur on Privacy report to the UN Human Rights Council in March 2020 provides recommendations for protecting against gender-based privacy infringements, which are also relevant in the Covid-19 context.[25]

8. Protection of vulnerable populations

[24] Please note that, in some contexts, anonymous data can be re-identified – and thus data protection and privacy risks remain.

[25] Specifically, the SR noted that privacy is a right that applies to all, irrespective of gender, and that gender identity is integral to personality and important to self-determination, dignity and freedom and intersects with ethnicity, indigeneity and that the right to privacy provides important protection against discrimination. The SR stated, "Establishing clear international directions on how to protect against gender-based privacy infringements, will help prevent the ongoing harms experienced by many individuals and communities round the world."

Data from and on certain segments of the population may place them at a greater risk of harm and human rights abuses or increase their discrimination, marginalization and ability to access services. This might be due to, *inter alia*, early or advanced age, diminished mental and legal capacity, disability, migration status, sex, gender identity, criminalization of identity, status or behaviour. Data from and about these populations should be collected, stored and used with due regard to their higher risk of harm, noting the importance of avoiding function creep and ensuring that the purpose of data collection remains specifically related to public-health-specific aims.

9. Right of redress

Populations should have a legal right to redress from relevant parties when harm was caused as a result of either data collected about them, or the way in which these data were collected, processed or used.

What to do when you need to create/use technology for Covid-19-related work

1. In the absence of general data protection regulations, use regional or other international frameworks, as well as health data privacy regulations.

While many countries have not yet adopted general data protection laws, some countries have strong privacy protection regulations related to health data. Where this is the case, governments could be advised to apply these regulations to all data collected for the Covid-19 response.

Furthermore, in the absence of national laws, governments can also refer to regional and international human rights frameworks, regardless of whether they have been ratified. For example, in ECIS, countries can be guided by the Council of Europe's privacy and data protection directives.

UNDP Country Offices can inform national governments that we adhere to the International Covenant of Economic, Social and Cultural Rights and the principles and practices of the UN Global Pulse[26] and interventions, such as mobile apps, developed to support national efforts should be in line with those principles and be subjected to relevant due diligence and impact assessment procedures (even if not legally required in the jurisdiction).

2. Create a data authorization framework.

As the COVID-19 pandemic is primarily a matter of public health, digital efforts to combat the pandemic should, as much as possible, be led by medical or health administration professionals. Clear rules should exist as to who can gather, access and use what data and when. This includes digital monitoring or enforcement of self-isolation and quarantining of individuals or groups of individuals known to have tested positive for the virus or who are suspected to be at risk of contracting the virus, e.g., living with a person that has tested positive. Access to Covid-19-specific, health-related data should be limited to those who need information to conduct treatment, research or otherwise address the crisis. Under no circumstances should non-health-sector public officials – such as managers of national population registers, police or other security forces – be in a position to conduct their own analysis of infection data

[26] Relevant links are in Annex II.

to profile or target either individuals or vulnerable minority groups. In general, state security services, such as police forces, should be working under the direction of public health officials in the containment and mitigation phase of the pandemic and be engaged only as a means to enforce quarantine violations.

3. Set purpose limitation and data minimisation practices in place.

Processing of personal data should be for the express purpose of responding to the public health crisis and should be:

- adequate – sufficient to fulfil the stated purpose of containment and mitigation of the pandemic;
- relevant – with a rational link to that purpose;
- limited to what is necessary – required for the public health containment and mitigation purpose.

In its Covid-19 guidance, OHCHR calls on states to ensure that "health monitoring and surveillance that tracks the behaviour and movements of individuals should be specifically related to and used for public health-specific aims and be limited in both duration and scope." [27] It further requests the implementation of "robust safeguards to ensure that such measures are not misused by Governments or companies to collect confidential private information for purposes not related to the public health crisis."

Data collected from patients who have tested positive for Covid-19 via digital interventions such as apps should be as minimally invasive as possible so that the apps, for example, are not allowed to ask for details on issues such as religion or ethnicity.

If data are used to identify people who defy quarantine orders, review the legal framework that is used to enforce disciplinary actions.

4. Include privacy and participation at the design stage.

The state could convene a task force with outside experts, including human rights and privacy experts and representatives of civil society, national human rights institutions and the health care community, to develop and support the data collection system for tracking and analysing Covid-19. This will be to ensure a transparent and inclusive design process and oversight of the data storage and use protocols.

When a UNDP Country Office is assisting in the development of a digital response such as an app or a software solution, privacy and confidentiality issues should be taken into account at the design phase of new services.[28] Good practices include:

- Ensuring that users' participation in the system is voluntary and that the user has the power to exit the system and destroy all data permanently;

[27] OHCHR, op cit.

[28] There are various technological solutions to maximize privacy if designed carefully in advance. For example, a facial recognition system does not always need to be connected to a database that identifies who the person is. Similarly, surveillance cameras exist that limit intrusiveness by automatically hiding certain information from video or by limiting access to different types of information obtained from the video.

- Use and publication of open source code, to enable public expert scrutiny of protocols;
- Publication of the operating protocols of the system, in particular in relation to the use of data, and risks such as hacking, the likelihood of false positives/negatives, etc.;[29]
- Ensuring that all data are stored locally, on the user's device (although systems may provide protocols for transfer to a government public health ministry, ideally with the user's consent);
- Non-publication of personal data;
- Non-publication of location data without explicit user consent. An app, for instance, should be location-blind by default; a user should be clearly asked for consent if the app wants to turn location tracking on.
- Just like with the data minimization principles, the choice of technology should be limited to the problem that it is necessary to solve. For example, when contact tracing is required, it is sufficient to use Bluetooth technology.

Local public-health officials and health care providers, where possible, should examine and contribute to the transparency provisions during the design phase of any form of tracking app.

5. Best practice through the procurement process.

For Country Offices procuring services from the private sector, best practice in procurement could include, for example, only working with partners willing to comply with data minimization practices and ensuring (contractually) that there is a plan and procedure for deleting data after they become irrelevant for Covid-19-related work.

In some rare cases, working with reliable international private sector partners *could* result in a better data privacy environment, as data will be managed by the private sector partner and not the national government. Risks should be carefully assessed and mitigated in such cases, including assessing whether data sovereignty laws mandate housing of data in-country and under state jurisdiction.

COs are also strongly encouraged to ensure interoperability of tools being developed and to guard against proliferation of apps that may detract from widespread adoption of an officially endorsed solutions.

6. Privacy codes of conduct for commercial holders of data

Commercial holders of data that can be used to combat the spread of the virus, such as telecom companies, should be made aware of their privacy and data protection obligations with regards to user data. Telecommunications ministries and other public licence granters should update and communicate relevant privacy and data protection regulations and remind telecom companies of their responsibilities during the pandemic, including restrictions on publishing 'contact tracking' data such as where mobile

[29] For an example see (in relation to Singapore's Trace Together app) *"BlueTrace: A privacy-preserving protocol for community-driven contact tracing across borders"* (last accessed 15 April 2020).

phones are known to have been in close proximity with each other for extended periods. The state could also consider temporary 'nationalization' of such data.[30]

7. Careful licensing of private sector digital innovations

Private sector digital innovations that arrive on the market at a time of public health crisis must be carefully examined before licensing, by relevant public licensing bodies, for commercial use. Biometric innovations that allow, for example, fever detection that could indicate the presence of Covid-19 symptoms, should not be in commercial use in those private sector companies that are deemed essential services during public 'lockdowns' without regulation as to their use.

8. Conduct mandatory human rights and privacy due diligence processes for every partnership and public procurement

Private sector actors that develop and implement systems related to Covid-19 should follow UNDP's as well as (if applicable) their own industry guidelines ensuring human rights due diligence and impact assessment to identify salient risks, avoid fostering or entrenching discrimination and respect human rights more broadly. This includes responsibilities of the private sector actors to create processes to monitor, mitigate and report on potential harms and to notify affected individuals. Additional guidance can be found in OHCHR's Guiding Principles on Business and Human Rights.[31]

Any engagement with technology companies should apply the UNDP Private Sector Due Diligence Policy, the UN Global Pulse Due Diligence Tools[32] and the UN Global Pulse Risks, Harms and Benefit Assessment Tool.[33]

9. Start a conversation about the need for general data protection regulation

As of March 2020, 143 countries have passed modern data protection regulations.[34] The number of Member States with enforcement mechanisms, via either empowered information commissioners or data ombudspersons, etc., is considerably smaller. Data protection and privacy laws should have clear exceptions that apply to public health crises to allow for greater use of digital data than usual, but that have 'sunset clauses' allowing for a return to normal once emergencies subside. Where those exceptions currently do not exist, they can be either legislated for by parliaments and other legislative bodies or issued by emergency decree.[35]

10. Look beyond digital tracking and surveillance

[30] For example, via taking remote management of such data and/or placing public health officials temporarily on the boards of such companies in the emergency phase of the pandemic and/or by placing public IT professionals on-site where companies gather, process and mine such data.
[31] https://www.ohchr.org/documents/publications/guidingprinciplesbusinesshr_en.pdf
[32] https://www.unglobalpulse.org/policy/due-diligence
[33] https://www.unglobalpulse.org/policy/risk-assessment/
[34] Egypt's Personal Data Protection Law is the most recent addition, as of February 2020.
[35] This is in line with the 2018 Supplement of the Global Commission on HIV and the Law, which states that "governments must establish legal protections to safeguard the privacy and confidentiality of social media users, digital health technologies, online healthcare records, electronic medical records and communications with healthcare providers."

The experience of many countries that appear to be achieving success in managing the epidemic (such as South Korea and Taiwan) demonstrates that digital tracking and surveillance measures need to be integrated as part of a wider public health strategy that includes improving testing capacities and supplying hospitals with more medical equipment. More importantly, some countries with effective responses (such as Singapore) have chosen to rely on consent-based approaches that support public health contact tracing and testing strategies, encouraging citizens to participate in the public health effort by downloading apps that store contact information on their phones but leave the user in control of the data.

For further information or support, please contact:

Human rights: Sarah Rattray (sarah.rattray@undp.org)
Legal identity, biometric data: Niall McCann (niall.mccann@undp.org)
Digital governance: Minerva Novero-Belec (minerva.novero-bele@undp.org)
Digital tools and innovations: Daria Asmolova (daria.asmolova@undp.org)
Regional Focal Points: Nicholas Booth (nicholas.booth@undp.org); Ainura Bekkoenova (ainura.bekkoenova@undp.org)

ANNEX I – Examples of digital responses

A quick scan shows that many Covid-19 response efforts involve using digital technologies. Below are some of the measures deployed by Member States' governments:[36]

a. Tracking and monitoring of known cases and 'at risk' contacts

- Using mobile phone geo-location data (derived mostly from repeater towers,[37] but in some cases directly from user devices) to trace where patients who have tested positive for Covid-19 have travelled since they began to show Covid-19 symptoms and for a number of weeks thereafter. Often, as part of the same approach, mobile phone geo-location data are used to 'contact trace' those persons known to have had substantive contact within a close space with a person who tested positive for Covid-19 (e.g., where two mobile phones are known to have been within 2 metres of each other for at least 30 minutes).[38] Registered users of these devices are then informed that they may have been exposed to the virus and are advised to self-isolate;[39]
- Using national ID systems to contact either close relatives of a person who tested positive for Covid-19 or persons living close to that person, to inform them that they have been exposed to the virus and to thus recommend self-isolation.

b. Enforcing quarantines

- Using mobile phone geo-location (either via the device itself or via third-party apps, such as Facebook) to enforce self-isolation or quarantine orders, either for a minimum of 14 days or indefinitely, for:
    - Persons known to have tested positive for Covid-19, but who have either not required hospitalization or who have recovered and no longer require hospitalization;[40]
    - Entire communities, regardless of whether any members of that community have tested positive for Covid-19;
    - Recently arrived travellers from out of country or from areas of a country known to have high rates of positive Covid-19 tests;[41]

---

[36] For a larger list of examples, see "Latest on coronavirus surveillance: How governments are monitoring citizens." https://news.trust.org/item/20200327085805-zcpnk

[37] "A cell site, cell tower, or cellular base station is a cellular-enabled mobile device site where antennae and electronic communications equipment are placed—typically on a radio mast, tower, or other raised structure—to create a cell in a cellular network." www.wikipedia.org

[38] "The Singapore 'TraceTogether' app will work by exchanging short distance Bluetooth signals between phones to detect other participating users in close proximity of 2 metres." https://news.trust.org/item/20200320123323-sfofe

[39] "In southern Kerala state, authorities have used telephone call records, CCTV footage, and mobile phone GPS systems to track down primary and secondary contacts of coronavirus patients. Officials also published detailed time and date maps of the movement of people who tested positive." https://news.trust.org/item/20200320083233-2okve

[40] For example, in South Korea, where "Prime Minister Chung Sye-kyun said the country will make self-isolation violators wear electronic wristbands since the number of cases of people breaching the self-quarantine in recent weeks has raised concerns." https://m-en.yna.co.kr/view/AEN20200411000500320

[41] "Hong Kong has said it has more than 20,000 bracelets ready for arrivals. […] A QR code in the bracelets is meant to pair with a smartphone app to identify those who break quarantine during the 14 days." https://news.trust.org/item/20200320081630-xekm6

- Persons who have consulted 'tele-medicine' or 'tele-doctor' services that have advised callers to self-isolate for a minimum of 14 days after symptoms of Covid-19 have been verbally identified.

- Using mobile phone apps to impose various forms of self-isolation or quarantine for individuals based on risk factors (such as increased body temperature as detected by hand-held digital readers) and imposed via colour-coded responses on digital devices placed in public areas (e.g., such as entry to public transport locations, etc.)[42]

c. Monitoring 'warning sign' health-related data

- Using private sector digital innovations, such as internet-connected body thermometers used by a statistically significant section of the public, to monitor 'warning signs' that would indicate the presence of possible Covid-19 symptoms (such as body temperature rates) that can not only assist public health officials in isolating geographical areas that suggest higher than usual presence of the virus, but also give evidence as to the effectiveness of social distancing measures.[43] Other private sector innovations (but not yet deployed on a mass scale) include adapting pre-existing biometric systems, such as facial recognition systems, to also detect fever, etc.[44]

d. Mass alerts and information

- Providing alerts, hospital information and preventative advice information in multiple languages via text messaging, in terms of services available to the public and mass messaging to all registered users.[45], [46]

e. Promoting medical distancing

Tele-medicine services are being rapidly rolled out to reduce unnecessary face-to-face interaction between patients and health care personnel. Tele-medicine takes some of the enormous pressure off the frontline hospital infrastructure. Tele-medicine is also preventing health care-related COVID-19 transmissions and protecting vulnerable and immuno-compromised patients and health personnel

---

[42] "Fuxuema, which translates as 'school resumption code', allows students to fill out their daily temperatures and obtain a colour-based QR-code, a type of barcode, on their mobile phones that would show their health status," Tencent said, "Embedded in Tencent's popular messaging app WeChat, the mini-app is similar to health code systems launched last month by Tencent and rival Alibaba Group Holding's Alipay which Chinese residents across the country now have to use to travel within and out of cities," https://news.trust.org/item/20200323100206-0m028

[43] The Singapore 'TraceTogether' solution puts the user in charge of the data but requires a public health official to activate it – at which point (with the user's consent) data is shared with the government.

[44] Biometricupdate.com: Fever detection and facial recognition systems launched to help prevent virus spread

[45] For example, New York City activated early on a text messaging service that only requires anyone to text "COVID" to its existing "692692" system (the service is used also for other case-specific situations, sending alerts and info including security advice such as during New Year's Eve), https://www1.nyc.gov/office-of-the-mayor/news/138-20/mayor-de-blasio-issues-state-emergency. The channel was noted at first to lack non-English alerts, which was immediately responded to, underlining a lesson for many global cities whose population include multilingual/multiethnic groups.

46 Singapore had been touted as impressive in its response to Covid-19, able to limit spread very quickly. Among efforts is its use of social media and messaging applications (apps) since late January. It deployed alerts and messages through the most-used app (WhatsApp), which involves the use of AI to generate translations into Singapore's four official languages. It has also enabled a mechanism to connect ministries to facilitate information sharing and coordination, and the ability to generate new mailing lists rapidly to reach target constituencies. https://govinsider.asia/innovation/singapore-coronavirus-whatsapp-covid19-open-government-products-govtech/

workers. (The WHO lists tele-medicine among essential services to strengthen health systems' response to COVID-19 policy.)

Some or many of the above measures have been, in different jurisdictions, implemented or monitored by either administrative hospital personnel, health ministry administrative personnel, community health personnel, local government officials, private sector companies (such as telecoms companies), state security forces, or a mixture thereof. In many cases, there have been *ad hoc* partnerships with private sector companies (often telecom companies), either on a voluntary basis or imposed by emergency legislation. In the latter cases, these have often been as part of a suite of 'state of emergency' rule-of-law changes that, in some countries, have involved the suspension of parliaments and other legislative bodies, the expansion of government by decree, and the imposition of restrictions on the constitutional right to judicial review of the emergency powers.

In some cases, these measures have largely been automated (e.g., automatic notification of registered mobile phone users that their device was in close proximity, for an extended period, to the device of a person known to have tested positive). In other cases, state officials, or volunteers operating in coordination with officials, have personally engaged in one-on-one 'contact tracing' of those who have had, or are suspected to have had, contact with persons known to have tested positive for Covid-19.

ANNEX II – Key Resources

1. UNSCEB's Personal Data Protection and Privacy Principles
2. Mandate of the United Nations Special Rapporteur on the Right to Privacy – Task Force on Privacy and the Protection of Health-Related Data: Recommendation on the protection and use of health-related data
3. UNDG's Data Privacy, Ethics and Protection: Guidance Note on Big Data for Achievement of the 2030 Agenda
4. UN Global Pulse Due Diligence Checklist and Questionnaire
5. UN Global Pulse Risks, Benefits and Harms Assessment Tool
6. Select approaches:
    - Government: European Commission recommendation on a common Union toolbox for the use of technology and data to combat and exit from the COVID-19 crisis, in particular concerning mobile applications and the use of anonymized mobility data
    - Civil Society: Recommendations on privacy and data protection in the fight against Covid-19
    - Academia: Decentralized Privacy-Preserving Proximity Tracing (DP-PPT)
    - Scientific and Technology Community: Pan-European Privacy-Preserving Proximity Tracing
7. Cyber security standards:
    - OWASP Top Ten
    - Guidelines on Hardening and Secure Coding for Web Applications **(internal use only, i.e., for UNDP-developed applications)**
    - System Acquisition, Development and Maintenance Standards **(internal use only, i.e., for UNDP-developed applications)**