Privacy International's submission on the working draft of the WHO's Pandemic prevention, preparedness and response accord

September 2022

Introduction

Privacy International (PI) welcomes the opportunity to provide written input on the working draft of the WHO's Pandemic prevention, preparedness, and response accord ("WHO CAII") published on 13 July 2022.[1] PI has sought to closely follow and engage with the discussions leading up to the draft CAII, despite the significant limitations to civil society participation in the process. In November 2021, PI was a signatory to the open letter calling on the World Health Assembly to put human rights at the forefront of the pandemic treaty.[2] In April 2022, PI made a written submission, and delivered an oral statement, to the WHO Intergovernmental Negotiating Body public hearing.[3]

This submission is based on our research and assessment of data-reliant and tech-intensive measures deployed by governments and companies in response to Covid-19 and its aftermath, which documented how these measures impacted people's fundamental rights and freedoms, including the right to privacy and other human rights.[4]

Below we make comments to specific provisions of the working draft and provide some general observations to inform the document and its approach as a whole.

Preamble

[1] A/INB/2/3, 13 July 2022
[2] Fish Hodgson, T., Habibi, R., Mason Meier, B., Sekalala, S., Seiderman, I., Falchetta, T., Schwarz, T., Tayler, L., Tait, S., Staberock, G., and Davis. S. Human Rights Must Guide a Pandemic Treaty, Health and Human Rights Journal, 20 November 2021. Available at: https://www.hhrjournal.org/2021/11/human-rights-must-guide-a-pandemic-treaty/
[3] Privacy International, PI's contribution to the first public consultation for an International Pandemic Treaty, 12 April 2022. Available at: https://privacyinternational.org/advocacy/4838/pis-contribution-first-public-consultation-international-pandemic-treaty
[4] See: Privacy International, Fighting the Global Covid-19 Power-Grab, Available at: https://privacyinternational.org/campaigns/fighting-global-covid-19-power-grab; Privacy International, Tracking the Global Response to Covid-19. Available at: https://privacyinternational.org/examples/tracking-global-response-covid-19

9. Lessons learnt

There are immense lessons to be learned from recent prior pandemics around the use of data and technology and in particular the impact they have on people and their rights. These include the West Africa Ebola outbreak (thereafter Ebola outbreak) in 2014, the 2015 Middle East Respiratory Syndrome (MERS) outbreak in South Korea, as well as from the recent Covid-19/SARS-CoV-2 pandemic (thereafter Covid-19 Pandemic).

For example, a report on the use of technology in response to the West Africa Ebola highlighted: "the significant legal risks posed by the collection, use, and international transfer of personally identifiable data and humanitarian information, and the grey areas around assumptions of public good." [5]

Whilst the Covid-19 pandemic is still on-going across the world, initial evaluations and studies have reflected on the role played by new technologies and data, and their impact on the fundamental rights and freedoms of all but in particular of those on individuals and communities already in vulnerable positions.[6] Echoing its position throughout the Covid-19 pandemic,[7] the United Nations has initiated a process to reflect on this very issue and has shared some initial recommendations that "human rights should be at the heart of tech governance", and on the need to mitigate harmful use of technologies.[8]

There is an urgent need to reflect on what role data and technology played in the response to the recent pandemics, what role it didn't play, where was it beneficial and where it created risks that those actors responsible were not equipped to identify in the first place and then mitigate. We must see concrete efforts to audit and evaluate the measures deployed during the Covid-19 and other recent pandemics.

The drafting of the WHO CAII must be informed and shaped by those lessons learned to ensure a good starting point founded in evidence-based audits and evaluations and prevent not only the replication but the codification of poor policies and practices in the future.

Part II. Objective(s), principles and scope

Article 4. Principles

[5] McDonald, S. M., Ebola: A Big Data Disaster - Privacy, Property, and the Law of Disaster Experimentation, March 2016. Available at: https://www.academia.edu/21348760/Ebola_A_Big_Data_Disaster

[6] Sekalala, S., Dagron, S., Forman, L., and Mason Meier, B., Analyzing the Human Rights Impact of Increased Digital Public Health Surveillance during the COVID-19 Crisis, Volume 22/2, December 2020, pp 7 – 20, 8 December 2020. Available at : https://www.hhrjournal.org/2020/12/analyzing-the-human-rights-impact-of-increased-digital-public-health-surveillance-during-the-covid-19-crisis/; Venkatasubramanian, K., The Human Rights Challenges of Digital COVID-19 Surveillance, Health Hum Rights. 2020 Dec; 22(2): 79–84. Available at: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7762890/

[7] WHO Director-General's opening remarks at the media briefing on COVID-19, 11 March 2020. Available at: https://www.who.int/director-general/speeches/detail/who-director-general-s-opening-remarks-at-the-media-briefing-on-covid-19---11-march-2020; OHCHR, Coronavirus: Human rights need to be front and centre in response, says Bachelet, 6 March 2020, Press Releases. Available at: https://www.ohchr.org/en/press-releases/2020/03/coronavirus-human-rights-need-be-front-and-centre-response-says-bachelet?LangID=E&NewsID=25668

[8] OHCHR, `, 1 September 2022. Available at: https://www.ohchr.org/en/stories/2022/09/human-rights-should-be-heart-tech-governance

We welcome the inclusion of the principles related to respect of human rights, equity, transparency, accountability, gender equality, non-discrimination and respect for diversity and rights of vulnerable populations.

We would recommend that the treaty in this article and elsewhere as relevant provide additional details in relation to these principles. This is particularly important given the gap between principles and general obligations provided for in Part III, and specific provisions provided for in Part IV. It is essential that these principles be presented as the foundation of this instrument and all associated obligations be articulated in a way that upholds them.

(1) Right to health: It is important that this principle reaffirms the right to health as provided for in Article 25(1) of the Universal Declaration of Human Rights and Article 12 of the International Covenant on Economic, Social and Cultural Rights. In particular, this principle should cover the multiple dimensions of the right to health as stated by the General Comment No. 14 of the Committee on Economic, Social and Cultural Rights to include the following interrelated and essential core components: availability, accessibility, acceptability and quality.[9] Ensuring the protection, promotion and respect of the right to health through the lens of these four components is crucial to ensure its fulfilment.

(3) Respect and protection of human rights: The obligations and responsibilities of States and other entities including the private sector, are already articulated and established in national, regional and international human rights instruments. In reaffirming these obligations, the principle should clearly articulate the need for a human rights-based approach including the core pillars of: (i) accountability, (ii) equality and non-discrimination, (iii) participation, (iv) the universality, indivisibility and interdependence of human rights as recognised by the WHO[10] and other UN agencies, as well as empowerment and transparency.[11]

(7) Accountability: PI welcomes the inclusion of an accountability principle. However, to provide effective guidance to states and other actors, this principle should clearly articulate what constitute effective accountability including: (i) defining the responsibilities of each party where multiple actors are involved - identifying obligations, duties and standards, and (ii) designing mechanisms enabling third parties to scrutinise and challenge each actor's conduct**.** States and other actors subject to obligations provided for in national, regional and international law must be held to account and demonstrate how they comply with their obligations. In addition, there must be independent oversight mechanisms in place to ensure compliance and effective and accessible access to effective judicial and non-judicial

[9] General Comment No. 14 (2000), E/C.12/2000/4, para. 12
[10] https://www.who.int/news-room/fact-sheets/detail/human-rights-and-health
[11] See: UN Statement of Common Understanding on Human Rights-Based Approaches to Development Cooperation and Programming (the Common Understanding) was adopted by the United Nations Development Group (UNDG) in 2003. https://hrbaportal.org/the-human-rights-based-approach-to-development-cooperation-towards-a-common-understanding-among-un-agencies/

remedies. Furthermore, States should provide ample space for civil society to be able to observe, denounce and challenge their policies and practices.

The accountability principle should also spell out the role of states in holding companies to account. As part of their obligations under international human rights law, State must protect against human rights abuses within their territory and/or jurisdiction by third parties, including companies.[12] This is particularly important in the context of pandemic preparedness and response, given the increased role industry plays in the field of digital health.[13] Many States outsource to companies the delivery of public health programmes in the form of Public-Private Partnerships (PPP), and industry is also setting an innovation agenda often promoting 'solutions' that rely on and data exploitation and support a surveillance capitalism model[14]. Non-state actors, such as industry, must be held to account and their activities effectively regulated. (More details in Section: Regulating industry and Public-Private Partnerships)

(14) Non-discrimination and respect for diversity: We welcome the inclusion of this principle. However, the factors of discrimination included therein should be expanded. For example, there is ample evidence of how migrant and refugee populations[15] were disproportionately affected by the Covid-19 pandemic, as well as members of the LGBTIQ+ community[16] in terms of access to healthcare but also limitations on their freedom of movement and ability to sustain their livelihood, amongst other curtailments. We therefore would recommend further grounds of discrimination be recognised and listed in this principle including gender and legal status, particularly as the principle (15) considers refugees and migrants to be vulnerable populations.

Part III. General obligations

General obligation 2

We welcome the obligation to be inclusive of **communities, civil society and non-State actors**. We would particularly urge that additional efforts be taken to ensure the involvement of CSOs and

[12] For an overview, see: https://www.ohchr.org/en/business-and-human-rights.
[13] Privacy International, Digital Health: what does it mean for your rights and freedoms, 8 November 2021, available at: https://privacyinternational.org/long-read/4671/digital-health-what-does-it-mean-your-rights-and-freedoms
[14] Privacy International, Challenging Corporate Data Exploitation, available at: https://privacyinternational.org/strategic-areas/challenging-corporate-data-exploitation
[15] See WHO, Promoting the health of refugees and migrants during COVID-19 pandemic, https://www.who.int/activities/promoting-the-health-of-refugees-and-migrants-during-covid-19-pandemic; Privacy International, Migration and Covid-19, https://privacyinternational.org/examples/migration-and-covid-19; and Privacy International, Covid-19 doesn't discriminate based on immigration status - nor should the Home Office, https://privacyinternational.org/advocacy/3490/covid-19-doesnt-discriminate-based-immigration-status-nor-should-home-office
[16] See report to the UN General Assembly of the UN Independent Expert on protection against violence and discrimination based on Sexual Orientation and Gender Identity, https://undocs.org/Home/Mobile?FinalSymbol=A%2F75%2F258&Language=E&DeviceType=Desktop&LangRequested=False; Statement by human rights experts on the International Day against Homophobia, Transphobia and Biphobia, 17 may 2020, https://www.ohchr.org/en/statements/2020/05/covid-19-suffering-and-resilience-lgbt-persons-must-be-visible-and-inform?LangID=E&NewsID=25884; and World Economic Forum, LGBTIQ people have been hit hard by COVID-19. Here's how we can provide support https://www.weforum.org/agenda/2020/07/covid-19-lgbtiq-our-response/

communities acting on behalf of and representing affected individuals given that individuals often have access to more limited resources and leverage than other non-state actors such as industry. In particular, we encourage the recognition of the role that can be played by organisations and groups from disciplines who may not yet be involved in global health and health-related policymaking such as groups working at the intersection of human rights and technology.

General obligation 3

It is imperative that the treaty elaborate on this obligation to ensure the following interconnected areas are addressed: (i) due diligence and effective enforcement of human rights obligations of Parties and (ii) the effective regulation of the use of data and technology by Parties, and (iii) the effective regulation of industry by Parties as a cross-cutting issue.

This recommendation is driven by our observation that governments' responses to the COVID 19 pandemic has often been predicated on introduction of new or poorly tested technologies and the exploitation of personal data, without human rights due diligence and effective enforcement of human rights obligations and responsibilities leading to short-sighted decision-making with little consideration of what is needed for an effective public health response and limited understanding of the impact on individuals and communities, in particular those in vulnerable positions.[17]

The treaty must also require that Parties have publicly accessible, clear, precise, comprehensive and non- discriminatory legal frameworks to protect, promote and respect human rights and to regulate the use of data and technology by governments as well as industry:

- where such frameworks currently do not exist, legislative processes must be taken as a matter of urgency to ensure that they are drafted and adopted.

- where such legal frameworks exist, their effectiveness and application must be assessed, and if needed strengthened to ensure they are transparent, effective, robust and capable to hold actors accountable.

These legal frameworks are needed not only to cover health and health-related sectors but also other sectors and actors as they relate to wider human rights obligations:

- in other sectors, e.g. immigration enforcement, border management, social protection, etc.

[17] See: Privacy International, Fighting the Global Covid-19 Power-Grab, https://privacyinternational.org/campaigns/fighting-global-covid-19-power-grab; and Privacy International, Tracking the Global Response to COVID-19, https://privacyinternational.org/examples/tracking-global-response-covid-19

- as part of wider regulation of the use of data and technology such as data protection, digital national action plans and strategies, etc.

- to regulate the involvement of non-state actors such as industry through effective frameworks to oversee and manage Public-Private Partnerships (PPP).

Part IV. Specific provisions/areas/elements/obligations

The list of specific provisions/areas/elements/obligations already included in the working draft are a good starting point, but they fall short of addressing the areas of concern in relation to the protection of individual human rights, and in particular to activities associated with the use of data and technology which we have outlined below.

Human rights-based approach to health

Any efforts to strengthen health systems using innovation and technology must adopt a human rights-based approach.

Digital health interventions are increasingly common, and whilst there is no doubt that technological advancements can assist to improve access to healthcare and to respond to emergencies, human rights should always be protected in the process.

This includes respecting and protecting the right to privacy, including the protection of personal data (See section on: *Effective protection of personal data*), as well as an array of other fundamental rights and freedoms which have been well-documented to be implicated with the use of health technologies, including the right to non-discrimination, amongst others.

As is accepted by the WHO, adopting a human rights-based approach requires the following:[18]ensuring the participation of affected populations and rights-holders in decision-making, considering and responding to power dynamics and factors of discrimination by accounting for the needs of those in the most vulnerable position, and take measures to tackle and prevent patterns of discrimination; ensuring that right-holders have opportunities to exercise their rights, ensuring that decision-making processes are transparent, and appropriately communicated to the public, and adopting accountability mechanisms which clearly outline roles and responsibilities of actors, put in place mechanisms to ensure compliance and enforcement as well as redress mechanisms.

[18] See WHO, Human rights and health, https://www.who.int/news-room/fact-sheets/detail/human-rights-and-health

Upholding human rights in times of emergency

Well before the Covid-19 pandemic, the WHO had emphasised the importance of human rights in an outbreak response noting that any restrictive measures must be: "in accordance with the law; pursue a legitimate aim; proportionate; and not arbitrary or discriminatory".[19]

Specifically when it comes to privacy and management of data in health emergencies, the WHO has articulated that security and confidentiality remain central pillars of any decision-making even within times of emergency, the as indicated in its policy on data sharing in the context of public health emergencies.[20]

The balance between protecting health and respecting human rights was emphasised at the beginning of the Covid-19 pandemic by the Director General[21]. The WHO further noted that "Human rights frameworks provide a crucial structure that can strengthen the effectiveness of global efforts to address the pandemic."[22] In relations to the use of new technologies, the WHO recognised the possible risk of abuse if adequate safeguards were not adopted including discrimination, violations of privacy, or for targeting people and communities for purposed beyond the pandemic response, and noted that: "All measures must incorporate meaningful data protection safeguards, be lawful, necessary, and proportionate, time-bound and justified by legitimate public health objectives.[23]

The Office of the High Commissioner for Human Rights (OHCHR) recognised that respect for human rights and ensuring an effective public health response of a pandemic are intrinsically linked: "Respect for human rights across the spectrum, including economic, social, cultural, and civil and political rights, will be fundamental to the success of the public health response and recovery from the pandemic."[24] Whilst some rights and freedoms are qualified and can be curtailed in limited circumstances for legitimate purposes these still need comply with principles of necessity and proportionality, and identify and respond to the risks the impact on people and their rights, especially those already in marginalised and precarious situations.[25]

[19] See: The Siracusa Principles on the Limitation and Derogation Provisions in the International Covenant on Civil and Political Rights. See also WHO, Addressing Human Rights as Key to the COVID-19 Response, 21 April 2020, https://www.who.int/publications/i/item/addressing-human-rights-as-key-to-the-covid-19-response

[20] WHO, Policy statement on data sharing by WHO in the context of public health emergencies, https://apps.who.int/iris/handle/10665/254440

[21] WHO. Director General, Media Briefing, 11 March 2020, https://www.who.int/dg/speeches/detail/who-director-general-s-opening-remarks-at-the-media-briefing-on-covid-19---11-march-2020

[22] WHO, Addressing Human Rights as Key to the COVID-19 Response, 21 April 2020, https://www.who.int/publications/i/item/addressing-human-rights-as-key-to-the-covid-19-response

[23] COVID-19 and Human Rights - We are all in this together, April 2020 https://unsdg.un.org/sites/default/files/2020-04/COVID-19-and-Human-Rights.pdf, page 15-16

[24] UN Office of the High Commissioner for Human Rights, Covid-19 Guidance, https://www.ohchr.org/en/covid-19/covid-19-guidance

[25] Sophia A. Zweig, Alexander J. Zapf,* Chris Beyrer, Debarati Guha-Sapir, and Rohini J. Haar, Ensuring Rights while Protecting Health: The Importance of Using a Human Rights Approach in Implementing Public Health Responses to COVID-19, Health and Human Rights Journal, Volume 23/2, December 2021, pp. 173-186, https://www.hhrjournal.org/2021/10/ensuring-rights-while-protecting-health-the-importance-of-using-a-human-rights-approach-in-implementing-public-health-responses-to-covid-19/

The WHO CAII should align itself with the existing international human rights law and commitments of the WHO with regards to protection, promotion and respect of human rights including the right to privacy, in pandemic prevention and responses, including in times of emergencies.

Respect and protection of the right to privacy

The WHO has also articulated its understanding and commitment to the protection of privacy in relations to digital health in its Global Strategy on Digital Health (2020-2025).[26] The strategy clearly acknowledges the potential risks for people, their data, and their enjoyment of fundamental rights, and calls for strong legal and regulatory bases to protect "privacy, confidentiality, integrity and availability of data and the processing of personal health data". The WHO's strategy indicates its commitment to incorporate lessons learned and mitigate ethical, legal and governance challenges "including data privacy and sharing and ensuring safety and protection of individuals within the digital health environment." These principles and commitments must inform decisions made around the deployment of digital health initiatives including in relations to pandemics.

Effective protection of personal data

As noted elsewhere in this submission, States must ensure that they have an effective legal and regulatory framework in place to effectively regulate the processing of personal data.[27]

Whilst various national and international governance frameworks are in place to regulate the processing of personal data[28] including in the health sector (such as comprehensive national data protection laws or sectorial laws), a global digital health framework in the form of comprehensive digital health strategies and other mechanisms is only “at a nascent stage”.[29]

The WHO and other UN entities reaffirmed the obligations on governments that any data processing activities “in the context of the Covid-19 pandemic should be rooted in human rights and implemented with due regard to applicable international law, data protection and privacy principles, including the UN Personal Data Protection and Privacy Principles.”[30] The WHO further emphasised the obligations of governments, but also other actors, to: “Ensure that safeguards are in place where new technologies are

[26] WHO, Global strategy on digital health, 2020-2025, https://www.who.int/docs/default-source/documents/gs4dhdaa2a9f352b0445bafbc79ca799dce4d.pdf
[27] See Privacy International, Data Protection Guide, https://privacyinternational.org/taxonomy/term/512
[28] Nearly 150 countries around the world have adopted comprehensive data protection laws to protect people and their data, and around 30 have initiated a legislative process, and have a bill in the process of being drafted. See: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1951416
[29] Nigel Cory, Building a Global Framework for Digital Health Services in the Era of COVID-19, available at: https://www.researchgate.net/publication/341735792_Building_a_Global_Framework_for_Digital_Health_Services_in_the_Era_of_COVID-19
[30] UN Joint Statement on Data Protection and Privacy in the COVID-19 Response, 19 November 2020 https://www.who.int/news/item/19-11-2020-joint-statement-on-data-protection-and-privacy-in-the-covid-19-response

used for surveillance in response to COVID-19, including purpose limitations and adequate privacy and data protections."[31]

Protecting personal data and communicating clearly with people about the purpose their data will serve, and how it will meaningfully contribute to an effective public health response to a pandemic is fundamental to ensure effective pandemic prevention and response. Failing to do so risks undermining the trust people will have in their own governments and others, as well as those assisting them.

Below we outline some areas of concern we have observed in relations to the processing of personal data for health purposes and in particular in public health emergencies.

Lack of recognition of the sensitive nature of health data

Progressive data protection laws explicitly recognise the special status of health data, by categorising it as "sensitive personal data" or "special category of data". This means that health data enjoys higher levels of legal protection, including limitations on the permitted grounds for processing it. It is also important that the higher protections extend to data that reveals sensitive personal data as through profiling and the use of proxy information, e.g. location data, it is possible for those processing data to infer, derive and predict sensitive personal data without having been explicitly declared as sensitive personal data.

In recognition of the sensitive nature of health-related data and the information which can be derived from it, important safeguards have been reaffirmed by a variety of stakeholders, including the WHO[32], when such data is being processed.[33]

The WHO CAII must recognise this too as it will help identify and frame the problems and risks the principles outlined in Article 4 and corresponding obligations to be imposed on Parties, and other actors, under Part III and Part IV, to mitigate these risks.

Reliance of poorly defined grounds for processing of personal data

Common grounds for processing personal data include "public interest" and "legitimate interest" but in both cases often there is a lack of definition and clarity around what they constitute. As a result of this lack of clarity, from the onset of the Covid-19 pandemic, we observed governments and other actors, including the private sector, resorting to these grounds for justifying their processing activities but

[31] COVID-19 and Human Rights - We are all in this together, https://unsdg.un.org/sites/default/files/2020-04/COVID-19-and-Human-Rights.pdf, page 20.

[32] Data principles, World Health Organization (WHO), August 2020; The protection of personal data in health information systems – principles and processes for public health, World Health Organization (WHO)/Europe, August 2021, https://apps.who.int/iris/bitstream/handle/10665/341374/WHO-EURO-2021-1994-41749-57154-eng.pdf?sequence=1&isAllowed=y

[33] Summary of activities and a recommendation on the protection and use of health-related data, Report of the Special Rapporteur on the right to privacy, United 74th session of the United Nations General Assembly, A/74/722, August 2019; Protection of health-related data - Recommendation CM/Rec(2019)2, Council of Europe, 2019; Health Data Governance: Privacy, Monitoring and Research, OECD Health Policy Studies, 2015

without articulating clearly what was the public or legitimate interest was, nor whether it met the test of necessity and proportionality.[34]

Another ground for processing personal data which may fall within the scope of the activities regulated by the WHO CAII (sections on research and development as well as information and knowledge sharing) and sometimes included in data protection frameworks is processing data for scientific, historical, or statistical purposes.[35]

Given the above, we recommend that the WHO CAII include obligations to Parties so that all grounds for processing of personal data are:

- Clearly defined and communicated to the data subject at the point of collection;
- subject to other common data protection safeguards to protect the rights and interests of the data subject, including fairness, transparency; and
- a data protection impact assessment which clearly considers any prejudice or adverse effect on individuals' rights.

Abuse and misuse of exemptions and exceptions

Common exemptions provided for in data protection law is public health, vital interests of others, public security, amongst others. However, national laws have often formulated these exemptions very broadly or provide blanket exemptions for some purposes or some public actors, thereby undermining the essence of the right to privacy and other human rights.

As previously noted by the WHO and other UN entities, states' obligations to effectively prevent, prepare and respond to public health emergencies does not provide them a blank check to disregard or undermine the rule of law and people's rights and freedoms.[36]

In addition to wider exemption noted above, some data protection laws may provide exceptions to certain principles and/or rights of individuals if certain conditions are met. For example, there are two common exceptions to the principle of purpose limitation which allow for further processing beyond the original purposes include: (a) with the consent of the data subject" and (b) "by authority of the law". These exceptions are often abused and misused.

[34] Privacy International, Extraordinary powers need extraordinary protections, 20 March 2020 https://privacyinternational.org/news-analysis/3461/extraordinary-powers-need-extraordinary-protections

[35] Regina Becker, Adrian Thorogood, Johan Ordish, Michael J.S. Beauvais, COVID-19 Research: Navigating the European General Data Protection Regulation, Originally published in the Journal of Medical Internet Research (http://www.jmir.org), 27 August 2020. Available at https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7470233/

[36] COVID-19 and Human Rights - We are all in this together, https://unsdg.un.org/sites/default/files/2020-04/COVID-19-and-Human-Rights.pdf, page 15-20.

In the case of (a), the concern is that in situation where there is a power imbalance for example such as having to consent to the processing of your personal to access a benefit such as vaccination or use of a service, e.g., biometric health system or contact tracing apps, it raises concerns about whether this constitutes informed, freely given consent, and the ability to opt-out and withdraw consent. In the case of (b), this has been used by governments and companies to justify data being used for other purposes (function/mission creep) and to allow for wide data-sharing arrangements by state bodies and institutions in the exercise of their functions relying on legal grounds of public interest. In terms of mission creep, the WHO warned that there was a risk that "the crisis can provide pretext of the crisis to adopt repressive measures for purposes unrelated to the pandemic".[37] Reports of the repurposing of contact tracing apps for law enforcement goals have emerged in various countries.[38] There were also examples of function creep with contact tracing apps used to enforce lockdown measures and control crowds.[39] Examples of data sharing practices included health data being shared with border officials as part of Covid-19 status verification processes at the border[40] or telecommunications companies entering into data sharing agreements with public authorities to share location data of their users.[41]

For these reasons it is essential to ensure that any exemptions and exceptions are:

- clearly defined and prescribed by law,
- respect individual's fundamental rights and freedoms,
- are necessary and proportionate measure in a democratic society, and
- are only applicable, where failure to do so prejudice the legitimate aim pursued.

Failure to properly define and limit these exemptions and exceptions will undermine public trust which is essential to instil public trust as well as compliance with public health policies developed by health institutions.

Regulating industry and Public-Private Partnerships

There are few instances where governments can design, deploy and maintain digital systems themselves. The complexity of these systems and the highly technical know-how required to create

[37] COVID-19 and Human Rights - We are all in this together, https://unsdg.un.org/sites/default/files/2020-04/COVID-19-and-Human-Rights.pdf, page 3

[38] Leaver, T. (2021, 16 June) Police debacle leaves the McGowan government battling to rebuild public trust in the SafeWA app, The Conversation. https://theconversation.com/police-debacle-leaves-the-mcgowan-government-battling-to-rebuild-public-trust-in-the-safewa-app-162850 ; DW. (2022, 11 January). German police under fire for misuse of COVID contact tracing app. DW. https://www.dw.com/en/german-police-under-fire-for-misuse-of-covid-contact-tracing-app/a-60393597; Ilmner, A. (2021, 5 January). Singapore reveals Covid privacy data available to police. BBC News. https://www.bbc.co.uk/news/world-asia-55541001

[39] La Capital. (2020, 23 March). Controlarán a quienes incumplieron elaislamiento con una App en sus celulares. La Capital. https://www.lacapital.com.ar/la-ciudad/controlaran-quienes-incumplieron-elaislamiento-una-app-sus-celulares-n2572740.html

[40] Privacy International, Covid-19 vaccination certificates: WHO sets minimum demands, governments must do even better, 9 August 2021, https://privacyinternational.org/advocacy/4607/covid-19-vaccination-certificates-who-sets-minimum-demands-governments-must-do-even

[41] Privacy International, Telecommunications data and Covid-19, https://privacyinternational.org/examples/telecommunications-data-and-covid-19

them has led to the growth of the 'government-industry complex' that manages and regulates social protection programmes, including healthcare. PI has documented this increase reliance on private companies to deliver public health services including in the context of the COVID 19 pandemic.[42] Companies of all sizes, all over the world have been pitching data-intensive products, services, and solutions. Examples included companies' involvement in developing contact tracing apps, without necessarily considering their impact on privacy/data protection,[43] digital identity companies providing vaccination status identification tools,[44] data analytics company offering health data management solutions to countries across the globe, without any transparency regarding what those entailed[45] and telecommunications companies are entering into data sharing agreements with public authorities[46] or even third party analytics companies[47] to enable tracking and location mapping.

This 'government-industry complex' has largely evolved in a regulatory void, and yet it is very likely that many of the measures enabled through it will be considered for the next pandemic given aspects were already deployed in prior pandemics and industry has continued to invest vastly in the health sector with Covid-19 providing them a boost of influence.[48]

Therefore, it is essential that the WHO CAII specifically provides for obligations for States to effectively regulate the role that industry should play in the health sector including in emergency responses, and the level of accountability and scrutiny they should be subject to. Such obligations must consider and respond to the breadth of activities by industry from the provision of digital health infrastructure to the management and processing of data such as data analytics, and the development of tools such as contact tracing apps. Similarly, these obligations must push States to re-assess the involvement of companies with diverse motivations and agendas such as surveillance companies and data brokers.

Any obligation and associated provisions included in the WHO CAII which are encouraging the participation of the private sector such as Point 4. (b) on technology and know-how transfer, and or encouraging the use of technology and innovation to strengthen health systems as per Point 3 must carefully consider how to regulate PPPs and generally the involvement of industry.

[42] Privacy International, Covid-19 response: Corporate Exploitation, 8 April 2020, https://privacyinternational.org/news-analysis/3592/covid-19-response-corporate-exploitation;
[43] Privacy International, Covid Contact tracing apps are a complicated mess: what you need to know, 19 May 2020, https://privacyinternational.org/long-read/3792/covid-contact-tracing-apps-are-complicated-mess-what-you-need-know
[44] Privacy International, The looming disaster of immunity passports and digital identity, 21 July 2020, https://privacyinternational.org/long-read/4074/looming-disaster-immunity-passports-and-digital-identity
[45] Privacy International, The Corona Contracts: Public-Private Partnerships and the Need for Transparency, 26 June 2020, https://privacyinternational.org/long-read/3977/corona-contracts-public-private-partnerships-and-need-transparency
[46] Privacy International, Telecommunications data and Covid-19, https://privacyinternational.org/examples/telecommunications-data-and-covid-19
[47] See Belgium: Telecoms location data to be provided to third-party analytics company, https://privacyinternational.org/examples/3488/belgium-telecoms-location-data-be-provided-third-party-analytics-company
[48] Privacy International, Digital Health: What does it mean for your rights and freedoms, 8 November 2021, https://privacyinternational.org/long-read/4671/digital-health-what-does-it-mean-your-rights-and-freedoms; The Business of a Better World, Decisions, Decisions, Decisions, https://www.bsr.org/reports/BSR-Decisions-Rights-Based-Approach-Tech-Data-Public-Health-Emergencies.pdf

Based on the United Nations Guiding Principles on Business and Human Rights, some of the minimum safeguards which need to be adopted to mitigate the risks of human rights abuses resulting from PPPs include:[49]

- ensuring transparency of these partnerships and the technologies they deploy;
- adhering to procurement processes which includes undertaking a comprehensive human rights due diligence;
- adopting of robust accountability mechanism with clear obligations, duties and standards that shall be imposed upon each actor of the relationship;
- demonstrating the legality, necessity and proportionality prior to any contracting and during the contracting relationship;
- sustained oversight of the deployment and results of a technology establishing relevant oversight mechanisms, that address the potential harms caused by the deployment of private technologies on affected individuals and communities;
- providing both non-judicial and judicial avenues for redress to affected parties by both the state and the company.

[49] Privacy International, Safeguards for Public-Private Surveillance Partnerships, https://privacyinternational.org/our-demands/safeguards-public-private-surveillance-partnerships