

GLOBAL INFORMATION SOCIETY WATCH 2021-2022

Digital futures for a post-pandemic world



ASSOCIATION FOR PROGRESSIVE COMMUNICATIONS (APC)
AND SWEDISH INTERNATIONAL DEVELOPMENT COOPERATION AGENCY (SIDA)

Global Information Society Watch 2021-2022

Digital futures for a post-pandemic world

Operational team

Valeria Betancourt (APC)

Alan Finlay (APC)

Maja Romano (APC)

Project coordination team

Valeria Betancourt (APC)

Cathy Chen (APC)

Flavia Fascendini (APC)

Alan Finlay (APC)

Leila Nachawati (APC)

Lori Nordstrom (APC)

Maja Romano (APC)

Project coordinator

Maja Romano (APC)

Editor

Alan Finlay (APC)

Assistant editor and proofreading

Lori Nordstrom (APC)

Assistant proofreader

Drew McKeivitt

Publication production support

Cathy Chen (APC)

Graphic design

Monocromo

Cover illustration

Matías Bervejillo



APC would like to thank the Swedish International Development Cooperation Agency (Sida) for their support for Global Information Society Watch 2021-2022.

Published by APC

2022

Creative Commons Attribution 4.0 International (CC BY 4.0)

<https://creativecommons.org/licenses/by/4.0/>

Some rights reserved.

Global Information Society Watch 2021-2022 web and e-book

ISBN 978-92-95113-52-7

APC-202211-CIPP-R-EN-DIGITAL-342

Disclaimer: The views expressed herein do not necessarily represent those of Sida, APC or its members.

Tech, data and the pandemic: Reflecting for next time

Alexandrine Pirlot de Corbion and Gus Hosein

Privacy International

<https://privacyinternational.org>

Introduction

Responding to a pandemic is more than just the mobilisation of the health system and adaptation of scientific research; the response is also a creature of the tools and measures available to respond.

Governments and companies chose to use this pandemic to test a series of new and innovative measures alongside the traditional ones. A pandemic is an extraordinary time and using available tech capabilities and data is common but can also be extra-ordinary. They can also provide the rubric for a post-pandemic future, institutionalising some practices and infrastructure for the next public health response, or the next emergency, or the “new normal” normalising surveillance and control of people and communities.

Context matters: A slightly different pandemic

Every virus and so every pandemic is unique. And the SARS-CoV-2 or “COVID-19” was indeed novel. Some of its unique aspects are worth noting.¹

While public health experts may find better terminology for capturing these, in our understanding these considerations help to explain the challenges of this particular pandemic:

- The virus was primarily airborne.
- You could be asymptomatic and still transmit the virus.
- You could be vaccinated and still transmit the virus to others.
- You could repeatedly become infected.
- The virus mutated in ways that could escape some elements of the deployed vaccines.

- Elements of the vaccines’ effectiveness may reduce over time.
- Booster vaccinations could be used to increase the body’s defences against the virus.

It’s also worth noting that none of this was known when the pandemic began, and it trickled in over the course of the pandemic. Whether through a lack of transparency, or the length of time scientific knowledge takes to develop and permeate, or the evolving nature of the virus itself, public health professionals and governments had to take decisions in the absence of complete knowledge. This is entirely understandable, and it was commendable that innovative solutions were sought.

However, as the pandemic became better understood, and now that we can begin to see its full nature, we must reflect on whether “innovative solutions” were sought because the underlying fabric of public health and welfare was so frayed from decades of under-investment and if there was an over-investment in shiny “innovative solutions” rather than sustainable, systemic, fair and people-centred solutions.

To a degree you can track some tech and data responses alongside the available knowledge of the time and see that the best available knowledge was used to decide the best available responses. Some responses, however, became disassociated with the emerging knowledge. Regardless, too many crossed the lines of ethics, the law and good tech practice into opportunism, repression and tech-solutionism.

A typology of responses

By reflecting on the implications of some of the measures deployed by governments, industry and other third parties,² we can begin to assess the

1 Hu, B., Guo, H., Zhou, P., et al. (2021). Characteristics of SARS-CoV-2 and COVID-19. *Nature Reviews Microbiology*, 19, 141-154. <https://doi.org/10.1038/s41579-020-00459-7>

2 Privacy International. (2022, 20 March). Extraordinary powers need extraordinary protections. <https://privacyinternational.org/news-analysis/3461/extraordinary-powers-need-extraordinary-protections>. For an outline of different tracking technologies used during the COVID-19 pandemic and their flaws, see Privacy International. (2022, 31 March). Covid-19: a tech post-mortem. <https://privacyinternational.org/explainer/4814/covid-2022-tech-retrospective>

scale of data processing activities that took place and continue today.³ This assessment can help us to understand the magnitude of the challenge we face and will continue to face to protect people and their rights.

Measures adopted by governments and enabled by industry

The decisions made by governments around the world varied as the pandemic evolved and was experienced in different ways at different stages. Nonetheless there were some common approaches and tactics.

Quarantining and lockdown enforcement

Quarantining was a top first response by governments. Once someone could be identified as having symptoms relevant to COVID and once tests were developed to identify someone as having COVID, governments would move them to quarantine.⁴ Eventually the virus spread, so governments reached to lockdowns as a public health response. Even after lockdowns ceased, quarantine requirements were imposed on individuals and groups following exposure (often arising from contact tracing), or upon the development of symptoms (which led to contact tracing) or for people who travelled. These sustained measures had tragic implications for people in vulnerable situations.⁵

In all these cases data and tech could be used, and in many cases, were used for quarantine enforcement. First, telecommunications data was sought from telcos to identify if someone was moving around when they did not have authority to do so due to quarantine or lockdown.⁶ A leading example of this was Israel, where the government tasked the Israeli security service Shin Bet to track

mobile phones to curb the spread of the virus.⁷ Similar attempts were made in Kenya,⁸ South Africa⁹ and Mexico.¹⁰ Other data sources were proffered by industry, including data held by data brokers and other data aggregators based on smart phone apps, leaking data to assess the extent to which there was public adherence to caution and lockdowns.

Governments then started check-ins (done by government contacting individuals or individuals reporting to authorities) and used police powers of generalised monitoring (e.g. CCTV, facial recognition, drones)¹¹ or stop and search powers to ensure that individuals were complying with orders.

Apps were sometimes used for quarantine enforcement, for example, in Abu Dhabi¹² and Myanmar.¹³ These could disclose location data through GPS or other automatic means, or compel an individual to report their location data manually.

Contact tracing

Contact tracing can be an essential public health surveillance response to a transmissible virus.¹⁴ If someone tests positive, contact tracing allows the ability to identify individuals who may have been exposed to that individual while they were contagious.

In this pandemic, particularly in the early stages when it was unclear how the virus was transmitted, governments scrambled to use vast amounts of data to undertake contact tracing.¹⁵ Some gov-

3 See: Sequera Buzarquis, M. (2020, 7 March). Las emergencias no deberían ser un cheque en blanco. *TEDIC*. <https://www.tedic.org/noesunchequeenblanco>; Memdutt, V. (2020, 14 April). COVID-19 Surveillance Infosheet! *Right2Know*. <https://www.r2k.org.za/2020/04/14/covid-19-surveillance-infosheet>; Digital Rights Foundation. (2020, 13 March). Protecting Your Rights During the Covid-19 Outbreak. <https://digitalrightsfoundation.pk/protecting-your-digital-rights-during-the-covid-19-outbreak>; Foundation for Media Alternatives. (2020, 15 March). Covid-19, public health, and privacy: The FMA Digital Rights Report. <https://fma.ph/2020/03/15/public-health-and-privacy-amid-covid-19-the-fma-digital-rights-report>; <https://www.alsur.lat/pt-br/projeto/observatorio-covid-19>; <https://privacyinternational.org/campaigns/fighting-global-covid-19-power-grab>

4 <https://privacyinternational.org/examples/quarantine-enforcement-and-covid-19>

5 Privacy International. (2020, 6 April). We must protect people in vulnerable situations during lockdown or quarantine. <https://privacyinternational.org/news-analysis/3588/we-must-protect-people-vulnerable-situations-during-lockdown-or-quarantine>

6 <https://privacyinternational.org/examples/telecommunications-data-and-covid-19>

7 BBC News. (2020, 27 April). Coronavirus: Israeli court bans lawless contact tracing. *BBC News*. <https://www.bbc.com/news/technology-52439145>

8 Olewe, D. (2020, 9 April). Coronavirus in Africa: Whipping, shooting and snooping. *BBC News*. <https://www.bbc.co.uk/news/world-africa-52214740>

9 Hunter, M., & Thakur, C. (2020, 3 April). Advocacy: New privacy rules for Covid-19 tracking a step in the right direction, but... *amaBhungane*. <https://amabhungane.org/advocacy/advocacy-new-privacy-rules-for-covid-19-tracking-a-step-in-the-right-direction-but>

10 Galán, V. (2020, 31 March). El Gobierno de la CDMX ordena el cierre de centros comerciales por emergencia sanitaria ante Covid-19. *Business Insider Mexico*. <https://businessinsider.mx/cdmx-ordena-cierre-centros-comerciales-covid-19>

11 AP News. (2020, 25 June). Asia Today: India to survey 29 million New Delhi residents. *AP News*. <https://apnews.com/article/virus-outbreak-india-ap-top-news-new-delhi-international-news-f34eacac3d01431ab5848bb3aa03fc3d>

12 Nasrallah, T., & Zaman, S. (2020, 3 April). Abu Dhabi launches smart app to monitor home-quarantined people. *Gulf News*. <https://gulfnews.com/uae/health/abu-dhabi-launches-smart-app-to-monitor-home-quarantined-people-1.70796153>

13 See: <https://privacyinternational.org/examples/3911/myanmar-launches-app-enforce-quarantine>

14 WHO. (2021). *Contact tracing in the context of COVID-19: Interim guidance*. <https://www.who.int/publications-detail-redirect/contact-tracing-in-the-context-of-covid-19>

15 <https://privacyinternational.org/examples/contact-tracing>; Privacy International. (2020, 19 May). Covid Contact tracing apps are a complicated mess: what you need to know. <https://privacyinternational.org/long-read/3792/covid-contact-tracing-apps-are-complicated-mess-what-you-need-know>

ernments would search data stores in geographic locations where a COVID-positive person was known to have been (e.g. CCTV, restaurant billings, and other data sets stored more centrally, such as financial transactions or transport data).¹⁶

Mobile phone apps were also developed.¹⁷ These apps could use mobile phone data to detect proximity with other individuals. Bluetooth was eventually the selected technology in most countries' apps, alongside a decentralised infrastructure using pseudonymised data.¹⁸

Concerns about the effectiveness of proximity tracing using Bluetooth technologies were coupled with longstanding privacy concerns of using telecommunications data to track individuals.¹⁹ Reports of the repurposing of contact tracing apps for law enforcement goals have emerged in Australia,²⁰ Germany²¹ and Singapore.²² There were also examples of function creep with contact tracing apps used to enforce lockdown measures and control crowds.²³

Furthermore, organisations around the world documented the lack of privacy safeguards built into the design and implementation of contact tracing apps, including our global partners in Colombia,²⁴

the Philippines,²⁵ Chile²⁶ and Peru,²⁷ while others reported a disproportionate negative impact on marginalised groups including women and minority groups, and the criminalisation of communities leading to discrimination and stigma.²⁸

Border management

Governments started closing borders in March 2020 when the World Health Organization (WHO) declared COVID-19 a pandemic;²⁹ and when they slowly reopened, surveillance was embedded in new processes for travellers. It is important to note that these additional measures were added to an already vast surveillance infrastructure at the border and beyond to monitor travellers.³⁰

Quarantining was often required for travellers. The use of "testing for release" became more commonplace as testing infrastructure improved. Testing prior to travel meant that government agencies and a myriad of private sector firms were starting to be custodians of vast amounts of personal data about travelling families, including custodians of their test samples and results. The travel industry also began to gain access to vast amounts of new sources of data on travellers, including their detailed biographical and family documentation (e.g. marriage certificates, birth certificates) to prove family composition to travel to some locations depending on restrictions.³¹

16 South Korea is often identified as the prime example of this more advanced form of contact tracing. See: COVID-19 National Emergency Response Center, Epidemiology & Case Management Team, Korea Centers for Disease Control & Prevention. (2020). Contact Transmission of COVID-19 in South Korea: Novel Investigation Techniques for Tracing Contacts. *Osong Public Health and Research Perspectives*, 11(1), 60-63. <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7045882>

17 <https://privacyinternational.org/examples/apps-and-covid-19>

18 Privacy International. (2020, 31 March). Bluetooth tracking and COVID-19: A tech primer. <https://privacyinternational.org/explainer/3536/bluetooth-tracking-and-covid-19-tech-primer>

19 BBC News. (2020, 27 April). Op. cit.

20 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>

21 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>

22 Illmer, A. (2021, 5 January). Singapore reveals Covid privacy data available to police. *BBC News*. <https://www.bbc.co.uk/news/world-asia-55541001>

23 La Capital. (2020, 23 March). Controlarán a quienes incumplieron el aislamiento con una App en sus celulares. *La Capital*. <https://www.lacapital.com.ar/la-ciudad/controlaran-quienes-incumplieron-el-aislamiento-una-app-sus-celulares-n2572740.html>

24 Labarthe, S., & Velasquez, A. (2020, 18 April). Covid apps in Colombia, Karisma's digital security and privacy evaluation. *Fundación Karisma*. <https://web.karisma.org.co/covid-apps-in-colombia-karimas-digital-security-and-privacy-evaluation>

25 Foundation for Media Alternatives. (2020, 8 July). Open letter to request for strong user privacy protections in the Philippines' COVID-19 contact tracing efforts. <https://fma.ph/2020/07/08/open-letter-to-request-for-strong-user-privacy-protections-in-the-philippines-covid-19-contact-tracing-efforts>

26 Derechos Digitales. (2020, 16 April). CoronApp: La inutilidad del atajo tecnológico desplegado por el Gobierno y sus riesgos. <https://www.derechosdigitales.org/14387/coronapp-la-inutilidad-del-atajo-tecnologico-desplegado-por-el-gobierno-y-sus-riesgos>

27 Morachimo, M. (2020, 14 April). Quince propuestas para mejorar la aplicación del Gobierno del Covid-19. *Hiperderecho*. <https://hiperderecho.org/2020/04/quince-propuestas-para-mejorar-la-aplicacion-del-gobierno-del-covid-19>

28 Davis, S. (2020, 29 April). Contact Tracing Apps: Extra Risks for Women and Marginalized Groups. *Health and Human Rights Journal*. <https://www.hhrjournal.org/2020/04/contact-tracing-apps-extra-risks-for-women-and-marginalized-groups>

29 <https://privacyinternational.org/learn/tech-border>; WHO. (2020, 11 March). WHO Director-General's opening remarks at the media briefing on COVID-19 – 11 March 2020. <https://www.who.int/director-general/speeches/detail/who-director-general-s-opening-remarks-at-the-media-briefing-on-covid-19--11-march-2020>

30 See for examples: Hosein, I. (2005). Transforming travel and border controls: Checkpoints in the Open Society. *Government Information Quarterly*, 22(4), 594-625. <https://doi.org/10.1016/j.giq.2006.01.002>; <https://www.privacyinternational.org/learn/migration-and-borders>

31 Read, J. (2020, 29 September). Will new travel technology invade your privacy? *National Geographic*. <https://www.nationalgeographic.com/travel/article/will-new-travel-technology-invade-your-privacy-coronavirus>

Certification

There was limited global harmonisation in the approach to both the use and purpose of COVID-19 certification documentation. The uses of the certificate varied considerably across the globe. The certificates could identify “immunity”, meaning that someone had previously been infected, or “vaccination” if they had received a vaccine, or if they had been tested recently.

Some governments, including Israel,³² France³³ and Italy,³⁴ among others,³⁵ required the mandatory provision of a certificate to allow access to public life and activities such as public venues like restaurants or cultural events. While others never fully developed a policy on their use,³⁶ and with the pandemic having evolved, other pending plans for certification have been dropped,³⁷ including for international travel in some instances.³⁸

In particular, the mandatory approach to COVID-19 certification raised some serious concerns in terms of discrimination and the impact on already marginalised communities in contexts where access to vaccination was unequal and remained problematic in many parts of the world.³⁹ These risks and harms were also highlighted by the WHO in its guidance and aligned with its position that such mandatory requirements should not be introduced,

at least in the context of international travel, “given that there are still critical unknowns regarding the efficacy of vaccination in reducing transmission.”⁴⁰

As time went on and boosters became deployed, some countries decided to extend the nature of the proof required. That is, your vaccine passport lost some of its “passport” capacity if you had not received more recent boosts. This was in theory to induce people into getting a third or fourth vaccination. But with equitable access to vaccination still being of concern, requiring certification of boosters remained highly controversial.⁴¹

Mass monitoring

Public health surveillance may involve wide-scale monitoring.⁴² Usually this is done with the knowledge and the consent of the patients, but rarely with people one level removed from them (i.e. contacts or others in proximity).

In this pandemic public health surveillance expanded in some new ways. Temperature checks on people entering buildings became more common.⁴³ This was a surprising development considering not everyone who had COVID necessarily was symptomatic, and not everyone with a temperature was necessarily carrying COVID.⁴⁴

Governments also sought to use and expand their existing mass surveillance tools for this pandemic.⁴⁵ This entailed population-level or geographic analyses using metadata, CCTV, and eventually drones⁴⁶

32 Holmes, O., & Kierszenbaum, Q. (2021, 28 February). Green pass: how are Covid vaccine passports working for Israel? *The Guardian*. <https://www.theguardian.com/world/2021/feb/28/green-pass-how-are-vaccine-passports-working-in-israel>

33 Chrisafis, A. (2021, 12 July). France mandates Covid health pass for restaurants and cafés. *The Guardian*. <https://www.theguardian.com/world/2021/jul/12/france-mandates-covid-health-pass-for-restaurants-and-cafes>

34 Giuffrida, A., & Henley, J. (2021, 24 November). Italy to tighten Covid rules for unvaccinated with ‘super green pass’. *The Guardian*. <https://www.theguardian.com/world/2021/nov/24/italy-poised-to-tighten-rules-for-unvaccinated-with-super-green-pass>

35 McDonagh, S., & Gallagher, T. (2021, 17 November). Green pass: Which countries in Europe require a COVID vaccine pass to get around? *Euronews*. <https://www.euronews.com/travel/2021/10/12/green-pass-which-countries-in-europe-do-you-need-one-for>

36 Jackson, M. (2021, 12 September). England vaccine passport plans ditched, Sajid Javid says. *BBC News*. <https://www.bbc.co.uk/news/uk-58535258>

37 Al Jazeera. (2022, 12 February). Israel PM announces end of vaccine ‘green pass’. *Al Jazeera*. <https://www.aljazeera.com/news/2022/2/17/israel-pm-announces-end-of-vaccine-green-pass>

38 Thackray, L. (2022, 30 June). The destinations that have scrapped all travel restrictions – regardless of vaccination status. *The Independent*. <https://www.independent.co.uk/travel/news-and-advice/countries-no-travel-restrictions-tests-unvaccinated-b2071371.html>

39 Ganty, S. (2021). The Veil of the COVID-19 Vaccination Certificates: Ignorance of Poverty, Injustice towards the Poor. *European Journal of Risk Regulation*, 12(2), 343-354. <https://doi.org/10.1017/err.2021.23>; Maombo, S. (2021, 22 November). Amnesty warns against mandatory vaccination approach. *The Star*. <https://www.the-star.co.ke/news/2021-11-22-amnesty-warns-against-mandatory-vaccination-approach>

40 WHO. (2021, 5 February). Interim position paper: considerations regarding proof of COVID-19 vaccination for international travellers. <https://www.who.int/news-room/articles-detail/interim-position-paper-considerations-regarding-proof-of-covid-19-vaccination-for-international-travellers>

41 United Nations. (2022, 10 March). High Commissioner for Human Rights: the Failure to Administer the COVID-19 Vaccines in a Fair and Equitable Manner is Prolonging the Pandemic. <https://www.ohchr.org/en/press-releases/2022/03/high-commissioner-human-rights-failure-administer-covid-19-vaccines-fair-and>

42 WHO. (2022, 14 February). Public health surveillance for COVID-19: interim guidance. <https://www.who.int/publications-detail-redirect/WHO-2019-nCoV-SurveillanceGuidance-2022.1>

43 Privacy International. (2020, 30 July). Infrared temperature screening. <https://privacyinternational.org/explainer/4111/infrared-temperature-screening>

44 UK Medicines & Healthcare products Regulatory Agency. (2020, 3 July). Don't rely on temperature screening products for detection of coronavirus (COVID-19), says MHRA. <https://www.gov.uk/government/news/dont-rely-on-temperature-screening-products-for-detection-of-coronavirus-covid-19-says-mhra>

45 do Carmo Barriga, A., Martins, A. F., Simões, M. J., & Faustino, D. (2020). The COVID-19 pandemic: Yet another catalyst for governmental mass surveillance? *Social Sciences & Humanities Open*, 2(1). <https://doi.org/10.1016/j.sshao.2020.100096>

46 Mok, O. (2020, 24 March). Authorities monitor MCO-compliance from the sky with drones. *Malay Mail*. <https://www.malaymail.com/news/malaysia/2020/03/24/authorities-monitor-mco-compliance-from-the-sky-with-drones/1849681>

and facial recognition⁴⁷ to identify the movement of people.⁴⁸ The private sector has been instrumental in instigating and pushing for many of these tools, as it already did before COVID-19.⁴⁹

The private sector embeds itself further into our lives

Building on years of lobbying and investment, and a propensity to identify opportunities to sell its products, industry was quick to identify this global pandemic as yet another hook to push up their sales, and reinforce their influence in many areas of our lives from our work to our education to intimate spaces such as our health needs.

The pandemic challenged the momentum that had been building as a result of a decade of policy making around the world aimed at reining in the power and dominance of industry. The result was worse than mediocre.⁵⁰ Below we outline various sectors where industry entrenched itself further as a result of the pandemic, with little scrutiny, transparency or accountability.

Education

While prior to the COVID-19 pandemic, there was already growing investment in the provision of information and communication technologies in the educational sector, known as “edtech”, particularly by the private sector, this expanded drastically during the pandemic to enable children and adults to pursue their education online for various periods of time over the course of the pandemic.

Primary, secondary and tertiary education across the world adopted emergency remote learning measures with the uptake of education technologies – extending into homes during closures, into

classrooms when reopened, and beyond.⁵¹ This urgency of the demand for remote learning tools opened an opportunity for private companies to sweep in and offer their solutions with limited or no due diligence mechanisms to consider and respond to the impact of their adoption. Some countries expanded pre-existing infrastructure, but for many such infrastructure was not in place.⁵² We saw the rapid uptake of virtual platforms like Zoom⁵³ and Blackboard,⁵⁴ the expansion of initiatives provided by companies like Google⁵⁵ as well as the use of open-source platforms such as Moodle and Canvas.

In addition to privacy concerns, this has raised concerns in terms of ensuring the right to education with the entrenchment of existing socioeconomic inequalities associated with an increased reliance on technologies which are not only unequally distributed, but distributed with uneven quality of access.⁵⁶

Health care

The data and tech industry had identified the health sector as a fertile ground for data exploitation well before the COVID-19 pandemic.⁵⁷

47 Roussi, A. (2020, 18 November). Resisting the rise of facial recognition. *Nature*. <https://www.nature.com/articles/d41586-020-03188-2>; Van Natta, M., Chen, P., Herbek, S., Jain, R., Kastelic, N., Katz, E., Struble, M., Vanam, V., & Vattikonda, N. (2020). The rise and regulation of the thermal facial recognition technology during the COVID-19 pandemic. *Journal of Law and the Biosciences*, 7(1). <https://doi.org/10.1093/jlbb/lbaa038>

48 Bacchi, U. (2022, 9 March). Pandemic surveillance: is tracing tech here to stay? *Thomson Reuters Foundation*. <https://news.trust.org/item/20220304092506-akyoc>

49 See: <https://privacyinternational.org/learn/public-private-surveillance-partnerships>; Privacy International. (2021, 18 November). Huawei and Surveillance in Zimbabwe. <https://privacyinternational.org/long-read/4692/huawei-and-surveillance-zimbabwe>; Privacy International. (2020, 25 June). Huawei infiltration in Uganda. <https://privacyinternational.org/case-study/3969/huawei-infiltration-uganda>

50 Privacy International. (2020, 8 April). Covid-19 response: Corporate Exploitation. <https://privacyinternational.org/news-analysis/3592/covid-19-response-corporate-exploitation>

51 See, for example: Digital Rights Foundation. (2021). *Virtual Learning and Privacy Amid COVID-19*. <https://digitalrightsfoundation.org/wp-content/uploads/2022/01/Virtual-Learning.pdf>; <https://cetic.br/pt/tics/pesquisa/2020/escolas/G1>; <https://www.worldbank.org/en/topic/edutech/brief/how-countries-are-using-edtech-to-support-remote-learning-during-the-covid-19-pandemic>

52 Muñoz-Najar, A., Gilberto, A., Hasan, A., Cobo, C., Azevedo, J. P., & Akmal, M. (2021). *Remote Learning during COVID-19: Lessons from Today, Principles for Tomorrow*. World Bank Group. <https://documents1.worldbank.org/curated/en/160271637074230077/pdf/Remote-Learning-During-COVID-19-Lessons-from-Today-Principles-for-Tomorrow.pdf>

53 Duball, J. (2020, 28 April). Shift to online learning ignites student privacy concerns. *IAPP*. <https://iapp.org/news/a/shift-to-online-learning-ignites-student-privacy-concerns>

54 Muñoz-Najar, A., Gilberto, A., Hasan, A., Cobo, C., Azevedo, J. P., & Akmal, M. (2021). Op. cit.

55 For example, Google Workspace for Education, which includes Google classroom. It was first introduced in Amazonas state, Brazil, in 2015; see: Repórter Parentins. (2015, 8 April). Governador José Melo formaliza parceria do Governo do Estado com Google para serviços tecnológicos educacionais. <https://reporterparentins.com.br/?q=276-conteudo-2657-governador-jose-melo-formaliza-parceria-do-governo-do-estado-com-google-para-servicos-tecnologicos-educacionais>; see also da Cruz, L. R., & Venturini, J. R. (2020). Neoliberalismo e crise: o avanço silencioso do capitalismo de vigilância na educação brasileira durante a pandemia da Covid-19. *Revista Brasileira de Informática na Educação*, 28, 1060-1085. <https://br-ie.org/pub/index.php/rbie/article/view/v28p1060>

56 UN Special Rapporteur on the right to education. (2020, 20 June). Right to education: impact of the coronavirus disease crisis on the right to education – concerns, challenges and opportunities. *A/HRC/44/39*. <https://www.ohchr.org/en/calls-for-input/reports/2020/report-impact-covid-19-crisis-right-education>; UNICEF. (2021, 29 April). Crianças de 6 a 10 anos são as mais afetadas pela exclusão escolar na pandemia, alertam UNICEF e Cenpec Educação. <https://www.unicef.org/brazil/comunicados-de-imprensa/criancas-de-6-10-anos-sao-mais-afetadas-pela-exclusao-escolar-na-pandemia>

57 Privacy International. (2021, 10 November). Why we need to talk about digital health. <https://privacyinternational.org/long-read/4674/why-we-need-talk-about-digital-health>

Since the start of the pandemic, companies all over the world have pitched data products, services and solutions to COVID-19 – from big tech to companies that might not be household names. Well-known software companies like Palantir invested in a COVID-19 response by offering health data management solutions to countries across the globe.⁵⁸

Furthermore, with the need at certain points in the pandemic to limit in-person interactions and limitations in reaching those in diverse geographic locations as a result of restrictions on movement, telemedicine experienced a global boost.⁵⁹ Diverse tools have been used, from real-time, video-based health consultations and advice, to health monitoring apps/software and sensor-based systems, among others.⁶⁰ As few governments develop their own software and hardware or infrastructure, industry has already played different roles, from providing digital health initiatives such as mass, centralised databases for patient management to the use of applications and other digital tools for the delivery of care.

While they have the tools and resources, with many having shaped their business models around data exploitation and surveillance, we need to ensure that whatever contributions companies make in the health care sector improve access to and quality of care while protecting people and their rights.⁶¹

Employment

Employees and workers were dramatically impacted by this pandemic, and then by government and employers' responses. The private sector swept in with their products, with many being deployed with very limited or no consideration for the risks associated with them for workers, their rights, and their well-being.⁶²

Remote working forced employers to expand or adopt a new digital infrastructure to enable their employees to work using online platforms for

communication, and cloud solutions to share documentation and information, among other tools to enable the day-to-day operations of their businesses.⁶³ As this evolved and grew, we saw a shift that led to measures focused on surveillance and constant monitoring of workers to keep track of performance and efficiency.⁶⁴

Another result of lockdown measures and other limitations on movement has been the boom in home delivery applications and other gig economy sectors such as transportation.⁶⁵ This is a sector where there has been unprecedented surveillance that gig economy workers are facing from their employers. We are all coming to finally recognise and listen to concerns around the labour rights of the gig economy workforce and how the experience of these workers is being shaped by platforms they have little or no control over.⁶⁶

Future proofing

We all experienced this pandemic, and we all have our own set of reflections about what worked or didn't. At Privacy International we worked with partner organisations across the world, engaged with governments, and worked with international organisations and industry as we all struggled through appropriate responses. Throughout we can say that much was missing: adequate public health resources and infrastructure, fairness in access, equality in rights and capability, trust and confidence. And yes, data about the virus.

Now, looking back from wherever we are within this pandemic, we are very concerned that governments and industry are only focusing on the problem of inadequate data. If that is the only lesson, then the calls for more data and tech will follow – which means more tech sector in our health care, more data sharing, and more exploitation. That will all come at the cost of increased social protection. And it will predicate future responses, arming public health responses to prioritise strict quarantine enforcement rather than helping people to care for themselves and others; coercion and compulsion

58 Privacy International. (2020, 6 May). (Sort of) Trust but Verify: Palantir Responds to Questions about its work with NHS. <https://privacyinternational.org/long-read/3751/sort-trust-verify-palantir-responds-questions-about-its-work-nhs>; see also: <https://www.palantir.com/covid19>

59 Mou, M. (2020, 22 October). Covid-19 Gives Boost to China's Telemedicine Industry. *Wall Street Journal*. <https://www.wsj.com/articles/covid-19-gives-boost-to-chinas-telemedicine-industry-11603379296>

60 Privacy International. (2021, 28 October). Telemedicine and data exploitation. <https://privacyinternational.org/long-read/4655/telemedicine-and-data-exploitation>

61 Privacy International. (2021, 8 November). Digital Health: What does it mean for your rights and freedoms. <https://privacyinternational.org/long-read/4671/digital-health-what-does-it-mean-your-rights-and-freedoms>

62 University of St Andrews. (2021, 22 November). Employer surveillance during COVID has damaged trust. *Phys.org*. <https://phys.org/news/2021-11-employer-surveillance-covid.html>

63 Rodriguez Contreras, R. (2021, 15 December). COVID-19 and digitalisation. *Eurofound*. <https://www.eurofound.europa.eu/data/digitalisation/research-digests/covid-19-and-digitalisation>

64 Privacy International. (2020, 7 May). Unlocking workplaces, virtually locking workers in. <https://privacyinternational.org/news-analysis/3757/unlocking-workplaces-virtually-locking-workers>

65 Bueno, C. C. (2020, 1 December). Pandemia, Tecnología y Trabajo. *Global Data Justice*. <https://globaldatajustice.org/gdj/191/>

66 Privacy International. (2021, 13 December). Managed by Bots: surveillance of gig economy workers. <https://privacyinternational.org/long-read/4709/managed-bots-surveillance-gig-economy-workers>

over public educational programmes; profiling, identification and rationing over open access to public health services.

In addition to the direct measures deployed to respond to the health crisis, there is a need to scrutinise what shifts occurred across sectors, from the delivery of health care, to employment settings and remote learning, in a moment of panic and urgency with few measures subject to the necessary deliberations. This is necessary before current problematic practices become the foundation of our day-to-day lives in which industry has been let in, but should now be showed the way out or at least put back in its place.

The COVID-19 pandemic showed how fragile our protection framework is when it comes to protecting

people, their rights and data. Governments and companies were too easily able to deploy digital initiatives with little scrutiny, limited transparency, and weak accountability.

Starting now and going forward, we must reflect on these lessons to identify where and how we must spend our energy to strengthen the protection of people and their data, and to hold governments, companies and other third parties to account across the human rights protection framework. This is critical in advocating for people's fundamental rights and freedoms, from privacy to the right to health, education, fair working conditions, non-discrimination, and freedom of movement, among others. There will be future emergencies. We must be ready.

DIGITAL FUTURES FOR A POST-PANDEMIC WORLD

Through the lens of the COVID-19 pandemic, this edition of Global Information Society Watch (GISWatch) highlights the different and complex ways in which democracy and human rights are at risk across the globe, and illustrates how fundamental meaningful internet access is to sustainable development.

It includes a series of thematic reports, dealing with, among others, emerging issues in advocacy for access, platformisation, tech colonisation and the dominance of the private sector, internet regulation and governance, privacy and data, new trends in funding internet advocacy, and building a post-pandemic feminist agenda. Alongside these, 36 country and regional reports, the majority from the global South, all offer some indication of how we can begin mapping a shifted terrain.

GLOBAL INFORMATION SOCIETY WATCH
2021-2022 Report
www.GISWatch.org