HHR
Health and Human Rights Journal

PERSPECTIVE

The Trojan Horse: Digital Health, Human Rights, and Global Health Governance

SARA L. M. DAVIS

The COVID-19 pandemic has massively accelerated a global shift toward new digital technologies in health, a trend underway before the crisis. In response to the pandemic, many countries are rapidly scaling up the use of new digital tools and artificial intelligence (AI) for tasks ranging from digital contact tracing, to diagnosis, to health information management, to the prediction of future outbreaks. This shift is taking place with the active support of numerous private actors and public actors. In particular, United Nations (UN) development agencies, such as the World Health Organization (WHO), are actively encouraging this trend through normative guidance and technical cooperation aimed at helping the governments of low- and middle-income countries to assess their needs for digital health, develop national digital health strategies, and scale up digital interventions.[1] At the same time, global health financing agencies, such as the Global Fund to Fight AIDS, TB and Malaria, are financing these technologies through aid to national health programs and through their own public-private partnerships. But in this major effort to spur low- and middle-income countries to race toward the digital future, are UN development agencies adequately considering the risks?

In 2019, UN Special Rapporteur on Extreme Poverty and Human Rights Phillip Alston cautioned that digital technologies could be a "trojan horse" for forces that seek to dismantle and privatize economic and social rights, undermining progress toward the Sustainable Development Goals (SDGs) instead of speeding it.[2] Similarly, in 2020, UN Special Rapporteur on Racism Tendayi Achiume warned that technology is shaped by and frequently worsens existing social inequalities.[3]

As this article explores, these and other serious social effects may be accelerated by the rapid scale-up of digital technologies in health. An enabling policy and legal environment that confronts these risks and judiciously plans for them should be a precondition to the scale-up of digital technologies, not an afterthought. As part of its normative and technical advice to governments on digital technologies and AI in health, WHO should be supporting governments in assessing risks and needs and in ensuring that these governments also receive the advice they need to put in place laws, policies, and governance mechanisms to protect and uphold human rights. But to date, the main equity and human rights risk that WHO and other UN development agencies appear to view with real urgency is the need to overcome the "digital divide"—inequitable access to digital technologies and internet connectivity that might undermine access to digital health for impoverished and marginalized populations. In June 2020, the UN Secretary-General warned

Sara (Meg) Davis, PhD, is a research fellow at the Graduate Institute of International and Development Studies, Geneva, Switzerland.

Please address correspondence to the author. Email: meg.davis@graduateinstitute.ch.

Competing interests: None declared.

that closing the digital divide is now "a matter of life or death."[4] While addressing the digital divide is a legitimate concern in an increasingly digital age, a disproportionate focus on this issue could itself become a trojan horse, a poisoned gift to low- and middle-income countries that legitimizes sweeping access for private actors and state power, while rolling back hard-won human rights protections.

This article explores four risks in particular: the expansion of state surveillance, the risk of malicious targeting, numerous challenges linked to the management of partnerships with powerful private companies, and the risks of scaling up digital interventions for which scientific evidence is weak.

A trojan horse for state surveillance

In 2013, the UN General Assembly adopted a resolution expressing concern over the negative impact of technological surveillance on human rights.[5] A series of reports by UN Special Rapporteur on the Right to Freedom of Opinion and Expression David Kaye highlighted the systematic use of technologies to violate privacy rights.[6] The COVID-19 response has intensified these concerns, as some states expand systems of surveillance that could later be utilized for political purposes.

Function creep has been highlighted as a risk whenever personal data is gathered.[7] The Global Commission on HIV and the Law has particularly warned of the risk of digitally collected biometric information being used by the police.[8] The proposed gathering of biometric data (such as fingerprints or iris scans) for an HIV study sparked specific concerns for marginalized and criminalized groups in Kenya—namely, sex workers, men who have sex with men, transgender people, and people who use drugs—about the use of the data to target individuals for arrest.[9]

China offers a cautionary example of this targeted use of biometric data. To manage the coronavirus, the Chinese government requires citizens to download an app from Alibaba, a US$500 billion e-commerce company. The app was developed in partnership with the police and uses a color code to identify those free to travel, at risk, or in need of immediate quarantine, based on data that includes travel history and time spent in proximity to others with the virus.[10] Subway stations use thermal scanners to check for high temperatures, incorporating facial recognition technology.[11]

These tools were developed by some of the same companies responsible for developing AI systems used to profile millions of Uighur Muslims.[12] The systems track individual communications, police records, patronage at mosques, and individual movements to identify people considered high risk and place them in forced labor camps.

Beijing now actively exports these surveillance technologies, through its Belt and Road Initiative, to over 60 countries as a form of development assistance.[13] In August 2020, the International Telecommunication Union's AI for Good Global Summit tweeted a promotional video praising China's use of artificial intelligence without mentioning related abuses.[14] WHO has also praised China's response to COVID-19 without mentioning related rights abuses.[15]

Some humanitarian aid agencies, such as the International Committee of the Red Cross, have developed policies strictly limiting the gathering and use of biometric data, aiming to prevent state and nonstate actors using data gathered for humanitarian purposes to target people for harm.[16] However, there is currently no agreed approach to the governance and use of biometrics and other sensitive data among normative agencies, such as WHO, and funding agencies, such as the Global Fund, which often provide advice to the same countries. In fact, WHO's draft digital strategy, approved in 2020, appears to contravene its own data protection policy, according to an analysis by the Third World Network.[17] To promote consistent and rights-respective governance, agencies that normally work together to provide technical support and funding to low- and middle-income countries on health interventions should also work together to establish a common bottom line with regard to privacy, surveillance, and policing in the name of health, including policies on biometrics (potentially using the the International Committee of the Red Cross's policy as a starting point); and

certainly, they should deplore China's use of technology and AI for abusive policing, not extoll it on social media as a model.

A trojan horse for malicious targeting

Security experts have documented the growing use of AI systems for malicious purposes, including to attack both digital security (through phishing attacks, speech synthesis for impersonation, automated hacking, and data poisoning) and physical security (attacks using autonomous weapons systems, using micro-drones, and subverting cyber-physical systems).[18] UN High Commissioner for Human Rights Michele Bachelet has warned of the abuse of digital technologies to attack individuals and groups.[19] There are now growing cyber attacks against medical facilities which take advantage of hospitals' growing dependence on digital systems.[20]

Even where states do not retain the data, data gathered by digital contact tracing apps could enter the public domain, exposing women, girls, and other vulnerable groups such as LGBTI+ people or stigmatized groups to risks of stalking, extortion, or violence.[21] In South Korea, for example , digital contact tracing app data was used to create a "coronamap" website showing the travel histories of anonymous confirmed patients and identifying them by gender and age; as this information was publicly accessible, individuals were accused of infidelity, fraud, and sex work, and some were the targets of online witch hunts aimed at identifying individuals who had spread the virus. Moreover, individual businesses were associated with COVID-19 transmission after they were identified through contact tracing, and some were targeted for extortion.[22] Privacy International has documented data-exploitative tactics used by some organizations to target women with misinformation about contraception and abortion.[23] The International Committee of the Red Cross and Privacy International have further found that mobile technologies leave digital trails that could be used to target individuals.[24]

The growing dependence of health systems on digital technologies and AI thus creates many new vulnerabilities, and as Achiume has noted, due to inequalities that already exist in our societies, the risks are greater for some groups than for others. Incidents such as those documented in South Korea could undermine public trust and make many people reluctant to download or use mobile health apps. This may even have been the case in Singapore, where early downloads of the coronavirus app TraceTogether flatlined at just 20% of the population, leading the government to step back from promoting its use.[25]

A trojan horse for the private sector

Public-private partnerships may significantly benefit private actors, raising questions about the appropriate use of taxpayer funds.

Shoshana Zuboff has shown how tech giants such as Facebook and Google have turned data into a source of profit through "surveillance capitalism."[26] Today, private companies of all sizes race to locate big datasets that they can either sell for profit or use to train and improve algorithms, developing profitable tools. However, the supply of big data in the Global North is not enough to meet the demand, and privacy regulations in Europe and North America are growing stricter, thanks to the European General Data Protection Regulation. Health systems in low-resource settings offer potentially vast, as-yet-untapped reserves of big data in countries with weaker regulatory controls.

Thus, the private sector has a strong interest in partnering with health agencies to roll out new AI-enabled digital health tools in low- and middle-income countries, thereby accessing big data that would be harder to access in countries with stronger regulation, a form of "data colonialism."[27] Private companies may benefit significantly from partnerships in which there is no immediate obvious financial gain.

These partnerships sometimes include companies with problematic track records. In 2018, the World Food Programme's five-year partnership with data-mining firm Palantir was criticized by civil society due to Palantir's history of collaboration with Cambridge Analytica, the Los Angeles

and New York Police Departments, Immigration and Customs Enforcement, and US intelligence agencies.[28] One internal Immigration and Customs Enforcement report revealed that Palantir data had been critical in locating and prosecuting the parents of immigrant children.[29] The World Food Programme issued a statement affirming that it would place controls on the use of data by Palantir, but critics continue to raise concerns about the risks for refugees and persons in displacement and to call for clearer standards for humanitarian programs.[30] In response to COVID-19, Palantir is now offering its services to public health agencies to track and analyze the spread of the coronavirus.[31]

A trojan horse for unsupervised experimentation

WHO's draft digital strategy argues that it hopes to "[build] a knowledge base … enabl[ing] testing, validating and benchmarking artificial intelligence solutions and big data analyses across various parameters and settings."[32] But is it ethical to promote the testing, validating, and benchmarking of unproven health interventions in developing countries?

WHO's systematic literature reviews of evidence for new digital technologies tend to be consistent in praising the promise these offer, while also highlighting the need for further implementation research.[33] WHO has acknowledged in its guidelines that the quality of evidence for digital health interventions is sometimes weak, yet it nonetheless recommends them.[34]

The Committee on Economic, Social and Cultural Rights' General Comment 14 on the right to health asserts that health facilities, goods, and services must be scientifically and medically appropriate and of good quality.[35] The rapid scale-up of new digital technologies, even those with promising pilots, should be promoted by WHO and financed by publicly funded agencies only if the evidence base is sufficient to justify bringing new tools to scale. Financing unproven digital interventions may leach resources away from interventions for which the evidence base is stronger—for example, harm reduction services, which are proven to work but are chronically underfunded.[36]

Conclusion

The digital strategies and guidance currently emerging from global health agencies unfortunately make only minimal reference to these and other human rights concerns.[37] The report from the UN Secretary-General's high-level panel on digital technologies set the tone with its emphasis on addressing the digital divide, recommending that "by 2030, every adult should have affordable access to digital networks, as well as digitally-enabled financial and health services, as a means to make a substantial contribution to meeting the SDGs."[38] The panel's recommendations on human rights protection were far less precise, calling only for "an agencies-wide review of how existing human rights accords and standards apply to new and emerging digital technologies."[39] A year later, the "agencies-wide review" has yet to be published.

Similarly, WHO's draft digital strategy and normative guidance to countries focus overwhelmingly on the promise, with little discussion of the risks discussed above.[40] The strategy's four principles focus on urging countries to commit to digital health, recognizing the need for an integrated strategy, promoting the appropriate use of digital technologies for health, and recognizing the need to address impediments faced by the least-developed countries, and they make little reference to the concerns raised by UN human rights experts.[41] The strategy was approved by the WHO Executive Board in February 2020 and was on the agenda for approval by the World Health Assembly in November 2020.[42]

Recognizing that trust and respect for human rights are critical to upholding the right to health and that it is crucial to ensure that the public feels secure in accessing health care, global health agencies such as WHO and the Global Fund should, following the Ruggie Framework, "know and show" that they have done due diligence in order to

identify, prevent, and address human rights abuses linked to digital technologies in health.[43] This includes the following:

- developing a common position across WHO, the Global Fund, and other UN development agencies on the risks linked to these technologies, and clearly committing to making respect for human rights standards a core principle of all strategies and guidance;
- integrating consideration of the above risks into normative guidance by WHO and UNAIDS and developing risk assessment tools for countries and donor agencies;
- integrating a robust approach to due diligence into ongoing technical assistance provided to low- and middle-income countries by such agencies as UNDP, UNAIDS, French 5%, and others to enable states to fully assess the track records of companies with which they do business;
- developing biometrics and data management policies that share consistent principles across UN health agencies and global health funders: commiting to and recommending the minimal use of biometrics, setting out legitimate uses of health and biometric data, committing to impact assessments for data processing, and setting out constraints on private sector access to health data; and
- consulting with civil society—particularly affected communities—to ensure their involvement in the development and rollout of these policies.

Ultimately, states bear the responsibility to protect human rights; but UN development agencies and global health financing agencies, through the evidence-based normative guidance and technical cooperation they provide and the power they exercise as funders of health interventions, have signficant influence on state decisions, and they cannot afford to be naiive. As holders of the purse strings for billions in taxpayer contributions, they must do all they can to ensure that international cooperation does more good than harm. Given that technologies used in health will only continue to evolve, it is critical that respect for human rights move to the center of digital health governance and not be left as an afterthought.

Acknowledgments

The research for this article was supported in part by a consultancy with the Joep Lange Institute. I am grateful for input from Joe Amon, Christoph Benn, Erika Castellanos, Kene Esom, Tabitha Ha, Allan Maleche, Bruna Martinez, Mike Podmore, Tony Sandset, Peter van Rooijen, Akarsh Venkatasubramanian, Nerima Were, Carmel Williams, and two reviewers.

References

1. See, for example, World Health Organization, Draft global strategy on digital health 2020–2025 (Geneva: World Health Organization, 2020); World Health Organization and International Telecommunication Union, Be he@lthy, be mobile (Geneva: International Telecommunication Union, 2014); Global Fund, "Private sector partners step up the fight to end AIDS, TB and malaria" (press release, October 9, 2019). Available at https://www.theglobalfund.org/en/news/2019-10-09-private-sector-partners-step-up-the-fight-to-end-aids-tb-and-malaria.

2. United Nations General Assembly, Report of the Special Rapporteur on Extreme Poverty and Human Rights, UN Doc. A/74/493 (2019).

3. Office of the United Nations High Commissioner for Human Rights, "Emerging digital technologies entrench racial inequality, UN expert warns" (press release, July 15, 2020). Available at https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=26101&LangID=E.

4. United Nations, "Digital divide 'a matter of life and death' amid COVID-19 crisis, SecretaryGeneral warns virtual meeting, stressing universal connectivity key for health, development" (press release, June 11, 2020). Available at https://www.un.org/press/en/2020/sgsm20118.doc.htm.

5. United Nations General Assembly, Res. 68/147, UN Doc. A/RES/68/167 (2014).

6. Human Rights Council, Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, UN Doc. A/HRC/41/35 (2019).

7. S. Davis and A. Maleche, "Everyone said no: Key populations and biometrics in Kenya," Health and Human Rights Journal (July 4, 2018).

8. Global Commission on HIV and the Law, Risks, rights and health: Supplement (New York: UNDP, 2018); p. 8.

9. KELIN and the Key Populations Consortium, "Everyone said no": Biometrics, HIV and human rights, a Kenya case study (Nairobi: KELIN, 2018).

10. A. Holmes, "China is reportedly making people download an Alibaba-backed app that decides whether they'll be quarantined for coronavirus," Business Insider (March 2, 2020). Available at https://www.businessinsider.nl/alibaba-coronavirus-chinese-app-quarantine-color-code-2020-3?international=true&r=US.

11. S. Yuan, "How China is using AI and big data to fight the coronavirus," Al Jazeera (March 1, 2020). Available at https://www.aljazeera.com/news/2020/03/china-ai-big-data-combat-coronavirus-outbreak-200301063901951.html.

12. M. Gira Grant, "The pandemic surveillance state," New Republic (May 8, 2020).

13. S. Feldstein, The global expansion of AI surveillance (New York: Carnegie Endowment for International Peace, 2019).

14. AI for Good Global Summit (@ITU_AIForGood), "What is #China's digital #health strategy? #AI #AiforGood" (August 19, 2020). Available at https://twitter.com/ITU_AIForGood/status/1296031059948318720.

15. World Health Organization, Report of the WHO-China joint mission on coronavirus disease 2019 (COVID-19) (February 16–24, 2020). Available at https://www.who.int/docs/default-source/coronaviruse/who-china-joint-mission-on-covid-19-final-report.pdf.

16. B. Hayes and M. Marelli, "Faciliting innovation, ensuring protection: The ICRC biometrics policy," Humanitarian Law and Policy (October 18, 2019). Available at https://blogs.icrc.org/law-and-policy/2019/10/18/innovation-protection-icrc-biometrics-policy.

17. Third World Network, "WHO: Draft global strategy on digital health threatens data sovereignty" (press release, February 6, 2020). Available at https://www.twn.my/title2/health.info/2020/hi200203.htm.

18. M. Brundage, S. Avin, J. Clark, et al., The malicious use of artificial intelligence: Forecasting, prevention and mitigation (Future of Humanity Institute, University of Oxford, Centre for the Study of Existential Risk, University of Cambridge, Center for a New American Security, Electronic Frontier Foundation, and Open AI, February 2018), p. 4. Available at https://arxiv.org/pdf/1802.07228.pdf.

19. M. Bachelet, "Human rights in the digital age" (speech to the Japan Society, October 17, 2019). Available at https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=25158&LangID=E.

20. Oxford Institute for Ethics, Law and Armed Conflict, Oxford statement on the international law protections against cyber operations targeting the health-care sector (May 2020). Available at https://law.yale.edu/sites/default/files/documents/pdf/Faculty/circulation_oxfordstatement_internationallawprotections_cyberoperations_healthcare.pdf.

21. S. Davis, "Contact tracing apps: Extra risks for women and marginalized groups," Health and Human Rights Journal (April 29, 2020).

22. Corona map: COVID-19 status map. Available at https://coronamap.site; N. Kim, "'More scary than coronavirus', South Korea's health alerts expose private lives," Guardian (March 6, 2020). Available at https://www.theguardian.com/world/2020/mar/06/more-scary-than-coronavirus-south-koreas-health-alerts-expose-private-lives.

23. Privacy International, A documentation of data exploitation in sexual and reproductive rights (April 21, 2020). Available at https://privacyinternational.org/long-read/3669/documentation-data-exploitation-sexual-and-reproductive-rights.

24. International Committee of the Red Cross, Digital trails could endanger people receiving humanitarian aid, ICRC and Privacy International find (December 7, 2018). Available at https://www.icrc.org/en/document/digital-trails-could-endanger-people-receiving-humanitarian-aid-icrc-and-privacy.

25. G. Goggin, "COVID-19 apps in Singapore and Australia: Reimagining healthy nations with digital technology," Media International Australia (August 14, 2020). Available at https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7429912.

26. S. Zuboff, The age of surveillance capitalism (London: Profile Books, 2019).

27. N. Couldry and U. Mejias, "Data colonialism: Rethinking big data's relationship to the colonial subject," Television and New Media (April 20, 2018).

28. G. Greenleaf, "Global data privacy laws 2019: 132 national laws and many bills," Privacy Laws and Business International Report 157 (2019), pp. 14–18.

29. "Palantir played key role in arresting families for deportation, document shows," Mijente (press release, May 2, 2019). Available at https://mijente.net/2019/05/palantir-arresting-families.

30. N. Raymond, L. Walker McDonald, and R. Chandran, "Opinion: The WFP and Palantir controversy should be a wake-up call for humanitarian community," Devex (February 14, 2019). Available at https://www.devex.com/news/opinion-the-wfp-and-palantir-controversy-should-be-a-wake-up-call-for-humanitarian-community-94307.

31. Palantir, Responding to COVID-19 (November 15, 2020). Available at https://www.palantir.com/covid19.

32. World Health Organization (2020, see note 1), para. 17.

33. H. Abaza and M. Marschollek, "mHealth application areas and technology combinations: A comparison of literature from high and low/middle income countries," Methods of Information in Medicine 56/7 (2017), pp. e105–e122; C. Agbo, Q. Mahmoud, and J. Eklund, "Blockchain technology in healthcare: A systematic review," Healthcare (Basel) 7/2 (2019), p. 56; B. Bervell and H. Al-Samarraie, "A comparative review of mobile health and electronic health utilization in sub-Saharan African countries," Social Science and

Medicine 232 (2019), pp. 1–16; G. Fontaine, S. Cossette, M. Maheu Cadotte, et al., "Efficacy of adaptive e-learning for health professionals and students: A systematic review and meta-analysis," BMJ Open 9/8 (2019), p. e025252; K. Henry, A. Wilkes, C. McDonald, et al., "A rapid review of eHealth interventions addressing the continuum of HIV care (2007–2017)," AIDS Behavior 22/1 (2018), pp. 43–63; C. Kemp and J. Velloza, "Implementation of eHealth interventions across the HIV care cascade: A review of recent research," Current HIV/AIDS Reports 15/6 (2018), pp. 403–413; N. Konduri, G. Bastos, K. Sawyer, and L. Reciolino, "User experience analysis of an eHealth system for tuberculosis in resource-constrained settings: A nine-country comparison," International Journal of Medical Informatics 102 (2017), pp. 118–129; D. Rhoads, B. Mathison, H. Bishop, et al., "Review of telemicrobiology," Archives of Pathology and Laboratory Medicine 140/4 (2016), pp. 362–370; J. Ross, F. Stevenson, R. Lau, and E. Murray, "Factors that influence the implementation of e-health: A systematic review of systematic reviews (an update)," Implementation Science 11/1 (2016), p. 146.

34. World Health Organization, Recommendations on digital interventions for health sytems strengthening (2019).

35. Committee on Economic, Social and Cultural Rights, General Comment No. 14, The Right to the Highest Attainable Standard of Health, UN Doc. E/C.12/2000/4 (2000), para. 12(c).

36. UNAIDS, Health, rights and drugs: Harm reduction, decriminalization and zero discrimination for people who use drugs (Geneva: UNAIDS 2019).

37. See, for example, World Health Organization (2020, see note 1); United Nations Development Programme, Future forward: UNDP digital strategy (New York: United Nations Development Programme, 2020); World Health Organization, Digital health for the end TB strategy: Agenda for action (Geneva: World Health Organization, 2015). By contrast, USAID's digital strategy does address human rights risks; see USAID, USAID's digital strategy (Washington, DC: USAID, 2020).

38. UN Secretary-General's high-level Panel on Digital Cooperation, The age of digital interdependence (New York: United Nations, 2019), p. 4.

39. Ibid., p. 30.

40. World Health Organization, Recommendations on digital interventions for health system strengthening; classification of digital health interventions v1.0, WHO/RHR/18.06 (2018); World Health Organization, Digital technologies: Shaping the future of primary health care, WHO/HIS/SDS/2018.55 (2018); World Health Organization, Global diffusion of eHealth: Making universal health coverage achievable (Geneva: World Health Organization, 2016); World Health Organization, WHO compendium of innovative health technologies for low-resource settings (Geneva: World Health Organization, 2015); World Health Organization, The MAPS toolkit: mHealth assessment and planning for scale (Geneva: World Health Organization, 2015); World Health Organization, Early detection, assessment and response to acute public health events: Implementation of early warning and response with a focus on event-based surveillance; Interim version (Lyon: World Health Organization, 2014); World Health Organization, National eHealth strategy toolkit (Geneva: World Health Organization, 2011); World Health Organization, mHealth: New horizons for health through mobile technologies (2011). Available at https://www.who.int/goe/publications/goe_mhealth_web.pdf.

41. World Health Organization (2020, see note 1), paras. 22–30.

42. World Health Organization, Data and innovation: Global strategy on digital health, EB146(15) (2020).

43. Office of the United Nations High Commissioner for Human Rights, Guiding principles on business and human rights. (New York: United Nations, 2011).