HHR
Health and Human Rights Journal

Analyzing the Human Rights Impact of Increased Digital Public Health Surveillance during the COVID-19 Crisis

SHARIFAH SEKALALA, STÉPHANIE DAGRON, LISA FORMAN, AND BENJAMIN MASON MEIER

Abstract

The COVID-19 pandemic has led policy makers to expand traditional public health surveillance to take advantage of new technologies, such as tracking apps, to control the spread of SARS-CoV-2. This article explores the human rights dimensions of how these new surveillance technologies are being used and assesses the extent to which they entail legitimate restrictions to a range of human rights, including the rights to health, life, and privacy. We argue that human rights offer a crucial framework for protecting the public from regulatory overreach by ensuring that digital health surveillance does not undermine fundamental features of democratic society. First, we describe the surveillance technologies being used to address COVID-19 and reposition these technologies within the evolution of public health surveillance tools and the emergence of discussions concerning the compatibility of such tools with human rights. We then evaluate the potential human rights implications of the surveillance tools being used today by analyzing the extent to which they pass the tests of necessity and proportionality enshrined in international human rights law. We conclude by recommending ways in which the harmful human rights effects associated with these technologies might be reduced and public trust in their use enhanced.

Sharifah Sekalala is an Associate Professor of Global Health Law at the University of Warwick, UK.

Stéphanie Dagron is a Law Professor at the Faculties of Law and Medicine at the University of Geneva, Switzerland.

Lisa Forman is a Canada Research Chair Tier 2 in Human Rights and Global Health Equity at the Dalla Lana School of Public Health at the University of Toronto, Canada.

Benjamin Mason Meier is an Associate Professor of Global Health Policy at the University of North Carolina at Chapel Hill, USA.

Please address correspondence to Sharifah Sekalala. Email: sharifah.sekalala@warwick.ac.uk.

Competing interests: None declared.

Introduction

The COVID-19 public health crisis is the first truly global infectious disease threat in over a century. The scale of the pandemic has deepened the imperative for policy makers to expand beyond traditional public health mechanisms of surveillance to use new technologies, including global positioning systems, cell phone apps, and facial recognition to control the spread of SARS-CoV-2. These new surveillance technologies highlight longstanding tensions in public health between individual rights and collective interests. They also fall at the interface of multiple contemporary trends: the reduction of privacy online, the private monetization of online data, the use of big data in policymaking, and the abuse of online surveillance by governments. These trends are viewed as creating "surveillance states" and new forms of "surveillance capitalism" with the capacity to erode human rights and undermine democracy.[1] This context is important when it comes to digital public health surveillance mechanisms for COVID-19, since historical and contemporary rights abuses of surveillance mechanisms erode public trust and the solidarity necessary for the widespread adoption and public health efficacy of such mechanisms.

Human rights standards have evolved to ensure that public health surveillance mechanisms, even in the context of a public health emergency, meet human rights standards of legality, necessity, and proportionality. These standards require that adequate safeguards be put in place to ensure that such surveillance mechanisms, whether they are digital or traditional, do not illegitimately restrict the human rights to health, life, or privacy, and are not abused for the purposes of state control. In this light, the increased use of blanket enforcement measures, such as mass-scale video surveillance, drones, facial recognition, and even large-scale attempts at data mining, raise significant human rights concerns.

In this article, we explore the human rights dimensions of how these new technologies are being used to address the COVID-19 pandemic, and in particular, the extent to which they are legitimate restrictions on a range of human rights, including the right to privacy, the right to health, and other social and economic rights. We argue that human rights serve two important functions in the context of public health surveillance: first, by offering an important framework for safeguarding the public from overreach, and second, by enhancing the efficacy of the mechanisms themselves to the extent that their use in democratic constitutional contexts relies on widescale consensual public opt-in. We begin with mapping the surveillance technologies being used in the wake of the COVID-19 crisis, before analyzing the evolution and potential human rights implications of these tools. In doing so, we analyze the extent to which surveillance tools meet necessity and proportionality criteria in international human rights law. At the same time, we acknowledge the functional limitations of this assessment—international human rights law primarily binds states that ratify its instruments, yet it is often private corporate actors who create and use these tools. We discuss to what extent this balancing of human rights and public health imperatives extends to such nonstate actors. We close with recommendations to mitigate the human rights effects of these technologies and increase public trust in their use.

Public health surveillance during COVID-19

Public health surveillance is the systematic collection, storage, usage, and dissemination of personal information to identify an outbreak and mitigate the spread of disease.[2] In light of the global spread of COVID-19, the World Health Organization (WHO) has stated that the main objectives of surveillance during this pandemic are

> *to enable rapid detection, isolation, testing, and management of cases, to monitor trends in COVID-19 deaths, to identify, follow-up and quarantine of contacts, to detect and contain clusters and outbreaks, … monitor longer term epidemiologic trends and evolution of SARS-CoV-2 virus.*[3]

In further guidance on public health surveillance

during the COVID-19 crisis, WHO has also argued that digital technologies may support rapid reporting, contact tracing, and data management.[4] The use of digital tools in public health surveillance is not unique to the COVID-19 crisis. During the outbreak of severe acute respiratory syndrome in 2003, Hong Kong identified clusters of disease using electronic data systems.[5] During the Ebola outbreaks in West Africa in 2014–2016, mobile phone data were also used to model travel patterns and increase the viability of contact tracing.[6]

The current COVID-19 crisis has come at a time of digital revolution, with huge growth in mobile phone and social media use, and sophisticated technologies that can support widespread public health surveillance.[7] Digital surveillance tools can far more easily enable governments to identify disease outbreaks and engage in case identification.[8]

Outbreak surveillance

Digital surveillance tools have revolutionized the way in which public health systems can identify and respond to outbreaks. Tools such as WHO's Go.Data use real time data to register cases and their contacts, facilitating the analysis of contact tracing data and chains of transmission to better understand epidemics.[9] Tools are often run by third parties, such as technology companies and research institutes, which then have the capacity to mine data through machine learning and crowdsourcing.[10] For instance, the private Toronto-based corporation Blue Dot reported the emergence of COVID-19 through its early detection system before WHO declared a pandemic.[11] This was accomplished through the use of big data, which used natural language processing and machine learning to cull data from hundreds of thousands of sources, including statements from official public health organizations, digital media, global airline ticketing data, livestock health reports, and population demographics.[12]

While these new innovative systems can provide quick and often informative data, they can also suffer from problems of accuracy due to sample bias, over-interpretation of findings, and fragmentation among competing systems that lack a centralized approach to data collection.[13]

Case identification

Early and rapid case identification is crucial during a pandemic for the isolation of cases and tracing of contacts in order to reduce disease transmission.[14] Digital technologies can supplement clinical and laboratory notification through the automated use of symptom-based case identification, accelerating reporting to public health databases.[15] During the COVID-19 crisis, digital tools for case identification have been used through online symptom reporting apps in numerous countries, such as Singapore, Malaysia, the UK, and South Africa. Such tools can easily be integrated within national databases.[16]

During this crisis, we are also seeing the increasing use of wearable technologies, such as bracelets, which enable public health authorities to check people's temperatures and other symptoms in order to ascertain whether they may be experiencing COVID-19 symptoms. Liechtenstein, for example, plans to roll out such bracelets to the entire population.[17] Sensors, including thermal imaging cameras and infrared sensors, are being deployed within public spaces in Taiwan and Singapore (and by private companies in the United States and Canada) to identify potential cases on the basis of symptoms such as temperature.[18] Several airports, bus shelters, and train stations have installed these technologies, although there are concerns about the number of false positives that these schemes could generate.[19]

The tracing of contacts, which is designed to reduce onward transmission, is part of the case identification strategy. Previously, states relied primarily on manual contact tracing—interviewing an infected person, tracking down the recent contacts that they could recall, and advising those people to self-isolate. However, given the high proportion of pre-symptomatic transmission for COVID-19 and the scale of national and global infections, it was argued that manual contact tracing would be too slow to stop the progression of infection through the population.[20] This led to the development of digital tools to support faster contact tracing, primarily through the use of mobile smartphones or

other wearable devices with geolocation capability. Mobile phone contact tracing apps can thus make contact tracing and notification instantaneous, since, by keeping a record of proximity events between individuals, it can immediately alert recent close contacts of diagnosed cases and prompt them to self-isolate.[21]

Human rights concerns raised by evolving surveillance technologies

During pandemics, public health surveillance is considered critical for averting and containing the spread of a disease. However, these public health data are often personally identifiable and sensitive and may reveal details about a person's lifestyle, behaviors, and health.[22] Thus, the evolution of such surveillance technologies has always been accompanied by rights-based concerns about how the data are used.

Discrimination against vulnerable and marginalized populations was entrenched by early surveillance efforts. For instance, nationalist governments employed public health surveillance to legitimize discriminatory public health policies against migrants during the Industrial Revolution. The rapid spread of diseases in urban centers was often attributed to racial minorities, whether Roma populations in Europe or Chinese immigrants in the United States.[23] For instance, the rapid spread of smallpox in San Francisco in 1876 was falsely attributed to Chinese Americans living in the city, leading to quarantine orders on the basis of race. Public health officials produced reports that blamed the outbreak on the refusal of Chinese Americans to assimilate into Western society, highlighting their deviance from white society to further stigmatization and justify discrimination.[24] Following from the genocidal horrors of World War II, with Nazi eugenics laws massively violating the rights of minority populations under the purported public health justification of "healing the state," countries came together under the postwar United Nations (UN) to codify protections of individual rights.

Nondiscrimination and equality would become core elements of international human rights law. Article 2 of the 1948 Universal Declaration of Human Rights (UDHR) states that every human being is entitled to all rights and freedoms "without distinction of any kind, such as race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status." Similarly, the 1966 International Covenant on Civil and Political Rights (ICCPR) and the International Covenant on Economic, Social and Cultural Rights (ICESCR) require state parties to guarantee the enjoyment of all rights without discrimination of any kind.

These human rights developments would also look to protect individual privacy, first in the UDHR and culminating in the ICCPR.[25] The ICCPR created a legal imperative for states to ensure that no one is "subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation."[26] In developing these ICCPR provisions, states debated the conditions under which it would be acceptable when facing a national crisis (such as a public health emergency) to limit or suspend individual rights and freedoms—such as the right to privacy—seeking to balance the responsibility to protect their citizens and the imperative to uphold civil and political liberties.[27]

UN member states came to recognize that "public health may be invoked as a ground for limiting certain rights."[28] Through the Siracusa Principles, a nonbinding document developed by nongovernmental organizations and adopted by the UN Economic and Social Council in 1984, scholars developed a set of principles to ensure that any limitations on civil and political rights occur only "in narrowly defined circumstances," holding that such human rights infringements may be made only under the following conditions: (1) when applied as a last resort; (2) when prescribed by law (that is, not imposed arbitrarily); (3) when related to a compelling public interest (for example, the protection of public health); and (4) when found to be necessary, proportional to the public interest, and without less intrusive or restrictive measures available.[29]

The Siracusa Principles have become central to understandings of human rights derogation in the field of "health and human rights" and critical to understanding how human rights law should align with global health governance pursuant to the International Health Regulations. Developed by states as an international legal framework to address public health emergencies, the International Health Regulations' purpose is to prevent, protect against, control, and facilitate public health responses to the international spread of disease, and they make surveillance central to guiding effective public health action against cross-border disease threats.[30] Balancing the societal benefit of public health surveillance against the state infringement of individual rights, the revised International Health Regulations (2005) for the first time incorporated human rights into infectious disease control, focusing on human rights considerations in disease surveillance. The regulations structure state responses to public health emergencies of international concern in ways that are commensurate with, and restricted to, public health risks and which avoid unnecessary interference with international traffic, trade, and human rights.

Concerns raised by digital health surveillance during COVID-19

The scale and complexity of digital health surveillance raises four main concerns for human rights, and these human rights concerns risk undermining the public health surveillance system due to the erosion of public trust.

First, the efficacy of digital tools for global health surveillance is questionable, since many of these tools are still in the experimental phase.[31] For instance, at least 40 countries are using contact tracing apps, but there is not yet sufficient evidence about their ability to mitigate the spread of disease.[32]

Second, the fact that third-party actors are creating, using, and storing data poses questions of accountability. While traditional public health surveillance involved primarily the state, the rise of emerging digital surveillance tools has led to the involvement of a large number of third-party private actors that have access to personal health data that could be exploited in ways that irreparably damage trust in public heath surveillance.[33] In the UK, for instance, private companies Serco, SITEL, and Amazon Web Services will all have access to users' data, and these data will reportedly be held for 20 years. It is currently unclear whether these companies will be allowed to privately benefit from the use of these data.[34]

Third, beyond threats to the general public, increased digital health surveillance may exacerbate specific harms to minority groups such as LGBTQ people and migrants. This may be in the form of increased violations to their rights of privacy, increased discrimination, and the reinforcement of inequalities. While aggregated location data can monitor population flows in real time, identify potential transmission hotspots, and give insight into the effectiveness of other public health interventions, such as travel restrictions, it can also harm vulnerable users by identifying their physical locations. This is extremely concerning given that a recent analysis of 50 COVID-19-related apps in the Google store showed that only 16 explicitly stated in their policies their intent to anonymize user data.[35] Minority groups are particularly at risk of abuse of privacy; for instance, contact tracing for a COVID-19 outbreak in South Korea led to homophobic abuse targeted at the South Korean LGBTQ community.[36] There are already reports that some minority groups have been disproportionately affected by COVID-19 and, in many places, are already less likely to seek health care due to a history of discrimination.[37]

Making private and public service provision contingent on downloading digital surveillance tools (such as contact tracing apps) could not only constitute a threat to personal autonomy but also be discriminatory toward already disadvantaged groups. For instance, employers may demand that staff download apps before being allowed into work, people may need these apps in order to use public services (such as health services), and landlords could demand that people download apps before being able to rent a property. These examples are all problematic, not just because they are coercive but also because they reinforce inequality, often ex-

cluding poor and vulnerable groups of people, such as migrants who may not be able to access or use the apps. In India, for instance, the contact tracing app Aarogya Setu has now become mandatory for all employees, rendering the concept of meaningful consent irrelevant.[38] In Singapore, employers are told to encourage all workers to download the TraceTogether app, but it is mandatory for certain groups of migrant workers, making them particularly vulnerable as they often have fewer rights than other citizens.[39] Many migrants in these countries, especially those employed in the informal sector, are often poor and on precarious contracts. Mandatory requirements to download and use such apps would mean that they have to buy newer models of smartphones which are expensive. The use of digital surveillance tools could also disproportionately affect some groups, such as those with lower socioeconomic status and those who are older and who may not have adequate internet access.[40] For instance, the Qatari contact tracing app EHTERAZ is another example of a mandatory app that requires users to have compatible smartphones, which is problematic when many citizens and migrant workers live in poverty. In Qatar, people who fail to download the app could face up to three years in prison and a fine of QR200,000 (US$55,000). Such impositions disproportionately affect the 88% migrant population in Qatar, exacerbating existing social inequalities.

Fourth, the use of digital health surveillance measures may lead to abuses by states and nonstate party actors if such measures become embedded in other processes different from their original purposes. The long-term nature of the COVID-19 crisis has led to fears that a new extended regime of health surveillance could entail permanent, intrusive surveillance, lasting well beyond the "temporary" measures justified by an "emergency" context.[41] Digital surveillance apps could be linked to comprehensive medical records and used to enable health care access. In Hangzhou, China, authorities have reportedly started to link data from surveillance apps to citizens' medical records. There are also reports that authorities in Shanghai are considering integrating a personal health index into an app, which will rank citizens on indicators such as how much they sleep, how many daily steps they take, and how much they smoke and drink.[42] These extensions lead to concerns that the ability to access public services could be tied to the app, thereby making it easier to deny health care and other essential services to members of the public.[43] Furthermore, the commercialization of health data drawn from long-term surveillance could also lead to discriminatory exclusions and differential pricing by insurance companies.

Digital tools could also be securitized in a way that exceeds legitimate public health objectives. Some data from public health surveillance tools have already been shared with security officials. The governments of Israel, Kenya, Mexico, and Turkey, among others, have reportedly used the COVID-19 pandemic as an opportunity to analyze telecommunications data under the guise of "contact tracing."[44] The Pakistani government has repurposed an anti-terrorism system designed by the country's spy agency to trace suspected COVID-19 cases.[45] There are dangers that some of these surveillance mechanisms will become structurally embedded as they did in the US War on Terror—a modern example of how emergency measures may be abused to become permanent fixtures within societies.[46]

Finally, abuses due to the misuse of data, privacy violations, and discrimination due to the uneven coverage and consequences of digital health surveillance measures might not only damage public trust in public health surveillance but also lead to fragmented responses caused by competing actors promoting different digital tools

Human rights obligations and digital surveillance

Under international human rights law, states are required to have robust public health surveillance measures in order to safeguard the rights to life and health.[47] In the case of COVID-19, these obligations are critical, as surveillance is necessary to break chains of transmission and learn as much as possible in order to be able to develop better medical interventions, drugs, and vaccines.

As discussed above, digital surveillance can threaten the right to privacy, as enshrined in international human rights law, beginning in article 12 of the UDHR and confirmed in article 17 of the ICCPR.[48] Article 8 of the European Convention on Human Rights also protects privacy.[49] The right to privacy has been interpreted as covering the compilation, storage, use, processing, and dissemination of data relating to private life.[50] Any restrictions to the right to privacy should be legal and non-arbitrary; necessary and proportionate; and compliant with other rights guaranteed in these human rights instruments.[51] The European Court of Human Rights has held that the mere storing of data relating to the private life of an individual would constitute a violation of the right to privacy; it does not matter whether the information is sensitive.[52] The Siracusa Principles recognize that public health may be invoked as a ground for limiting certain rights (such as privacy) in order to allow a state to deal with a serious threat to the health of the population or individual people. Human rights derogations under the Siracusa Principles would need to meet three criteria: legality, necessity, and proportionality.[53] We will explore how the problems posed by digital tools stack up against these criteria below.

Legality

All restrictions to privacy must be non-arbitrary and prescribed by law.[54] The UN Human Rights Committee, which is mandated with monitoring and implementing the ICCPR, has argued that in order for law to be non-arbitrary, any interference provided for by the law should be in accordance with the aims and objectives of the ICCPR and reasonable in the particular circumstances.[55] In order to comply with legality, personal data must be processed in a transparent manner. Transparency is important within human rights discourse because it enables people to seek meaningful consent, monitor how data are used, and seek redress in instances where there are perceived violations of human rights.[56] Many governments have been accused of a lack of transparency. For instance, governments need to better explain what apps do, what data they collect, where they store the data, and the benefits that apps give to the general public. For example, the Indian government has been criticized for enabling the data collected from its contact tracing app to potentially be used by any government agency for other purposes.[57] Therefore, states and data organizations must be clear about how they will use personal data. In Israel, the High Court of Justice found that digital surveillance during the COVID-19 pandemic, which used national security legal authority for the Ministry of Health to implement the digital tracking of individuals, was illegal because it was conducted under an executive order and lacked the scrutiny that would have been present through legislative approval.[58]

Necessity

In order to limit rights through the use of digital technologies, states must show that the limitations are "strictly necessary," in that they must respond to a pressing public or social need.[59] WHO has acknowledged that surveillance measures are necessary to "limit the spread of disease, enable public health authorities to manage the risk of COVID-19, and thereby enable economic and social activity to resume to the extent possible," as well as to "monitor the longer-term trends of COVID-19 transmission and the changes in the virus."[60]

While there is excellent evidence that digital outbreak response tools are more efficient at providing epidemiological data for disease detection, the evidence on whether digital surveillance tools for contact tracing are actually effective remains inconclusive.[61] Some modelling suggests that digital health surveillance is necessary because the rate of transmission for COVID-19 is so rapid that manual contact tracing would be inadequate, but more data are needed to prove the efficacy of the tools.[62] The urgency of alleviating the pandemic does not remove the test of necessity, which requires proper scientific validity and accuracy.[63]

Proportionality

Under the principle of proportionality, the limitation on human rights must be commensurate to the aim. Measures must therefore be timebound and purpose-limited to the specific aim of preventing

the spread of infectious diseases. It follows that any digital health surveillance that goes beyond public health surveillance would fail the proportionality test. This view was also taken by the UN General Assembly when it considered the indiscriminate mass surveillance by the UK and US governments in the wake of the September 11 attacks. The subsequent UN resolution stated that "surveillance and/or interception of communications … as well as the collection of personal data, in particular when carried out on a mass scale, may have [a negative effect] on the exercise and enjoyment of human rights."[64] The European Court of Human Rights has been more expansive on the concept of mass state surveillance, holding that legal discretion granted to the state to enact surveillance cannot be unfettered.[65] In practice, this means that surveillance laws must not include blanket provisions, must be clear, and can be used only for a legitimate aim in order to ensure that the individual is protected from arbitrary interference.

To meet the test of proportionality, data should be used only for legitimate public health surveillance purposes, such as prevention of disease through the tracking and monitoring of patients with COVID-19. Determining what amounts to a legitimate public health surveillance purpose may sometimes be complex. Under the proportionality test, data could legitimately be shared across government agencies for health-related purposes or used to perform targeted interventions, such as reaching out to people who are at risk of getting COVID-19, if they have informed consent from users. However, it is clear that many digital health surveillance tools rely on broad consent, which may legally allow data to be used for future purposes. In order for this broad consent to meet the requirements of informed consent and maintain public trust, the use of future applications should still be transparent, and there should be publicly accessible mechanisms that can enable participants who download health apps to scrutinize the way in which their data are being used even after they have consented.

Digital health surveillance data may legally be used for enforcement purposes. For instance, test and trace data used to enforce quarantines and isolations serves a legitimate public purpose. Nevertheless, using data for enforcement would be considered human rights compliant only if done through a process that is transparent, nondiscriminatory, and time limited in order to help local authorities identify those at risk. Using criminal sanctions for enforcement would only legitimate and proportionate if used as a last resort.

Recommendations

This article has illustrated that new digital surveillance tools violate a number of human rights, such as the rights to privacy, freedom of movement, and health, in addition to committing several specific rights violations against vulnerable groups, such as migrants, LGBTQ populations, and the elderly. For digital surveillance tools to comply with human rights, they should be evidence based, contribute to a comprehensive public health surveillance system, include sunset clauses, be nondiscriminatory, and ensure mechanisms for greater transparency and accountability, including those aimed at nonstate actors such as private companies.

Evidence-based measures

To meet the criterion of necessity, states should insist on conducting rigorous pilot studies and risk assessments to ensure accurate, evidence-based decision-making.[66] Additionally, states should take advantage of national and regional evidence frameworks for digital health technologies.[67] WHO and regional bodies, such as the European Union, have started to give technical guidance about digital surveillance tools, but so far they have focused primarily on contact tracing apps; moving forward, they should also consider the wide range of additional digital surveillance tools that states may be using to monitor and control people.[68]

Additionally, a greater reliance on evidence would compel states to show that they cannot achieve the goal of preventing the spread of COVID-19 through "less restrictive means," including decentralized data within contact tracing apps or nontechnological measures. Some govern-

ments are using centralized approaches for contact tracing, in which data are stored on a central server managed by the authority that carries out the processing of the data. Under this model, once an individual comes into contact with an infected person, the state is notified and has the power to enforce quarantines and sanctions. Taiwan, for example, uses smartphone location tracking to detect and sanction quarantine violations.[69] However, other governments are opting for a decentralized approach in which most data are stored locally on an individual's phone, with the user having more control over how their data are shared with authorities.[70] Apple and Google are partnering with countries to promote the adoption of such a decentralized approach.[71]

Integrated public health surveillance measures

Digital technologies for surveillance must be integrated into the public health surveillance ecosystem. For instance, digital tools that offer symptom tracking or contact tracing must be followed by rapid testing, isolation or quarantine, treatment, and follow-up where necessary.[72] South Korea and Singapore have successfully introduced contact tracing apps to support large teams of manual contact tracers as one of many measures, including strict isolation of cases and quarantine.[73]

Temporality

States must ensure that digital health surveillance does not become a new norm. Given the risks to privacy, states must include a sunset clause to any laws that allow digital public health surveillance, which agrees ahead of time what data they are collecting, how long they should collect the data for, and when the permission to collect this data will expire. For instance, some states, such as Macedonia, have allowed users the power to delete all of their data after 14 days. Others, such as Australia, have made a provision for contact data stored on a device to be automatically deleted after 21 days.[74]

Nondiscrimination

To meet the criteria for legality, necessity, and proportionality, digital technologies must not be discriminatory. Digital health technologies can very easily collect large amounts of data about entire populations, with identifying markers such as race, ethnicity, gender, and sexual identity. Wrongly used, these data can lead to the stigmatization of already excluded minority or marginalized groups. Therefore, states have a human rights obligation to ensure that data from digital technologies are not misused at the expense of such groups.

Although there is an increasingly widespread use of digital technology, there is still unequal coverage, which may exclude vulnerable groups such as those who are poor or older people whose phones may not have the technology to support certain digital technology functions such as proximity tracing.[75] Thus, states should ensure that in opting for digital technologies, they are not excluding large parts of the population as this could affect access to health care services and heighten health inequalities.

Transparency and accountability

States relying on public health surveillance need to ensure that their digital public health surveillance follows a rights-based approach to transparency and accountability mechanisms. This would involve increased participation from a diversity of end users in the design and rollout of apps, independent oversight through civil society organizations, increased research into the human rights effects of these apps, and greater accountability for the holders of data, including third parties. For instance, in Italy, all of the data from public health surveillance tools is controlled by the Ministry of Health, and the government has committed to ensuring that data are not resold or used for commercial purposes. Some of these data "may be shared to facilitate scientific research, but only after its complete anonymisation and aggregation."[76]

Greater transparency also enables citizens to seek judicial scrutiny and appropriate remedies, particularly in the case of human rights violations. Transparency through strong multilateral and multistakeholder review frameworks is necessary to hold governments accountable where the use of contact tracing apps fails to meet the requirements

of international human rights law. Currently, there are some examples of domestic review processes that have managed to overturn excessive government surveillance during the COVID-19 pandemic. In Slovakia, the Constitutional Court declared the provisions of a newly amended telecommunications law passed in haste to be unconstitutional. The amendments sought to permit state authorities to access telecommunications data for the purposes of contact tracing; however, the provisions were struck down for being insufficiently clear and for lacking safeguards against misuse.[77]

Accountability for how data are used at the national level can be facilitated through formal mechanisms, such as national human rights action plans, which offer a structured and practical approach to strengthening the realization of human rights through public policy. National human rights action plans could focus on the ways in which state actors are using digital surveillance tools to establish whether human rights abuses are taking place. The Universal Periodic Review (UPR) is a unique process that involves a review of the human rights records of all UN member states. As a state-driven process under the auspices of the Human Rights Council, the UPR provides each state the opportunity to declare what actions it has taken to improve the human rights situations in its territory and to realize its human rights obligations. This process has been recognized as a useful tool for achieving greater state compliance with the right to health.[78] The role of civil society actors in both of these processes could ensure greater scrutiny of the human rights impact of digital health surveillance at the national level.

Lastly, there is an increased need for empirical research in this area, especially in areas where data may be subject to commercialization or deanonymization in the future.

Human rights obligations of third-party actors

Most digital surveillances involve third-party actors such as technology firms. Although states are the primary duty-holders under international law, there has been some consensus that nonstate actors such as private corporations "have duties to prevent human rights abuses …. where they maintain close connections with potential victims or potential perpetrators."[79] This broadens the scope of corporate responsibilities to ensure that firms' actions do not, however inadvertently, contribute to the systematic denial of human rights.[80] In 2011, the UN Human Rights Council endorsed a framework—the *Guiding Principles on Business and Human Rights*—allocating responsibility to corporations for human rights violations.[81] The Special Representative of the Secretary-General on business and human rights thereafter released a framework in which he argued that the state had the duty to protect against human rights abuses by third parties, including businesses; private actors had the duty to respect human rights; and there was a need for more effective remedies. The *Guiding Principles* articulated the idea that corporate responsibility extended to all internationally recognized fundamental human rights and that it was necessary to distinguish the specific responsibilities of corporations from the responsibilities of states.[82] The responsibility to respect involves effectively "doing no harm." This goes beyond a passive responsibility and can entail taking positive steps.[83] Discharging the responsibility to respect human rights requires that private companies carry out due diligence. For companies engaged in digital surveillance, this means that, just like states, they too need to consider whether digital surveillance tools meet the criteria of legality, necessity, and proportionality.

Due to the nonbinding nature of the *Guiding Principles*, the nature and extent of these responsibilities—as well as their consequences on private actors—are still contested.[84] The complex responsibilities of private companies involved in digital surveillance would benefit from specialist guidance from the UN human rights system, including human rights treaty bodies and Special Procedures mandate holders such as Special Rapporteurs.

Conclusion

Numerous digital tools are currently being used by states and private actors for public health surveillance in response to COVID-19. Many of these

tools raise human rights concerns about privacy, autonomy, and nondiscrimination. To comply with human rights law, it is important that digital tools pass the tests of legality, necessity, and proportionality for the legitimate restriction of rights.

For digital surveillance tools to comply with human rights, six key considerations should be considered. In the absence of compelling evidence about the efficacy of digital surveillance tools, states should ensure that they are evidence-based and focus on the least restrictive measures, such as decentralized contact tracing. States must ensure that digital surveillance tools are used to complement a comprehensive public health surveillance system and used in conjunction with measures such as testing, tracing, quarantining, and treatment. Any regulations to promote digital health surveillance should include sunset clauses and ensure that there is no discrimination against vulnerable groups. Additionally, states should ensure mechanisms for greater transparency and accountability, including those aimed at preventing nonstate actors such as private companies from violating human rights.

There is growing evidence that private companies need to respect human rights obligations by carrying out due diligence, which would require them to analyze whether digital tools meet the requirements of legality, necessity, and proportionality. The increased role of private corporate actors, who have less robust obligations than those borne by states, is concerning in digital health surveillance, and there is an urgent need for international human rights bodies to provide updated guidance on how private actors can be held accountable for human rights violations.

Acknowledgments

The authors are members of the Global Health Law Consortium, a collaborative interdisciplinary research initiative focused on advancing global health law. We are grateful to Belinda Rawson for her excellent research assistance. Additionally, we are grateful to two Global Health Law Consortium members, Gian Luca Burci and Stefania Negri, who commented on earlier versions of this paper, as well as the two anonymous reviewers who made some excellent and thought-provoking comments that helped us refine our arguments.

References

1. K. Chen, "No place to hide: Edward Snowden, the NSA, and the U.S. surveillance state," *Intelligence and National Security* 32/6 (2017), pp. 868–871; S. Zuboff, *The age of surveillance capitalism: The fight for a human future at the new frontier of power* (London: Profile Books, 2019).

2. L. O. Gostin, *Public health law and ethics: A reader*, 2nd edition (Oakland: University of California Press, 2010), p. 285.

3. World Health Organization, *Global surveillance for COVID-19 caused by human infection with COVID-19 virus: Interim guidance* (March 20, 2020), p. 1. Available at https://apps.who.int/iris/bitstream/handle/10665/331506/WHO-2019-nCoV-SurveillanceGuidance-2020.6-eng.pdf?sequence=1&isAllowed=y.

4. World Health Organization, *Digital tools for COVID-19 contact tracing* (June 2, 2020), p. 1. Available at https://apps.who.int/iris/handle/10665/332265.

5. G. M. Leung, A. J. Hedley, L. Ho, et al., "The epidemiology of severe acute respiratory syndrome in the 2003 Hong Kong epidemic: An analysis of all 1755 patients," *Annals of Internal Medicine* 141/9 (2004), pp. 662–673.

6. A. Wesolowski, C. O. Buckee, L. Bengtsson, et al., "Commentary: Containing the Ebola outbreak—the potential and challenge of mobile network data," *Public Library of Science Currents* 29/6 (2014).

7. S. Kemp, *Digital 2020: Global digital overview* (DataReportal, 2020); D. S. W. Ting, L. Carin, V. Dzau, et al., "Digital technology and COVID-19," *Nature Medicine* 26 (2020) pp. 459–461; S. Whitelaw, M. A. Mamas, E. Topol, et al., "Applications of digital technology in COVID-19 pandemic and response," *Lancet Digital Health* 2/8 (2020), pp. e435–e440.

8. World Health Organization, *Digital tools for contact tracing annex: Contact tracing in the context of COVID-19* (June 4, 2020).

9. World Health Organization, *GO.DATA user guide* (March 31, 2020), p. 11. Available at https://apps.who.int/iris/bitstream/handle/10665/332255/WHO-2019-nCoV-Go.data_manual-2020.2-eng.pdf.

10. See C. E. Koppeschaar, V. Colizza, C. Guerrisi, et al., "Influenzanet: Citizens among 10 countries collaborating to monitor influenza in Europe," *JMIR Public Health Surveillance* 3/3(2017), p. e66.

11. B. McCall, "COVID-19 and artificial intelligence: Protecting health-care workers and curbing the spread," *Lancet Digital Health* 2/4 (2020), pp. e166–e167.

12. C. Stieg, "How this Canadian start-up spotted coronavirus before everyone else knew about it," *CNBC* (March

3, 2020). Available at https://www.cnbc.com/2020/03/03/bluedot-used-artificial-intelligence-to-predict-coronavirus-spread.html.

13. J. Budd, B. S. Miller, E. M. Manning, et al., "Digital technologies in the public-health response to COVID-19," *Nature Medicine* 26 (2020), pp. 1183–1192.

14. World Health Organization, *WHO Director-General's opening remarks at the media briefing on COVID-19 - 16 March 2020* (March 16, 2020). Available at https://www.who.int/dg/speeches/detail/who-director-general-s-opening-remarks-at-the-media-briefing-on-covid-19---16-march-2020.

15. Budd et al. (see note 13).

16. Singapore Government, *Singapore COVID-19 symptom checker* (2020). Available at https://sgcovidcheck.gov.sg/.

17. Privacy International, *Liechtenstein adopts biometric electronic bracelets for nationwide health monitoring*, (April 16, 2020). Available at https://privacyinternational.org/examples/3724/liechtenstein-adopts-biometric-electronic-bracelets-nationwide-health-monitoring.

18. W. Naude, "Artificial intelligence vs COVID-19: Limitations, constraints and pitfalls," *AI and Society* (2020), pp. 1–5.

19. B. J. Quilty, S. Clifford, S. Flasche, et al., "Effectiveness of airport screening at detecting travellers infected with novel coronavirus (2019-nCoV)," *EuroSurveillance* 25/5 (2020).

20. M. Parker, C. Fraser, L. Abeler-Dörner, et al., "Ethics of instantaneous contact tracing using mobile phone apps in the control of the COVID-19 pandemic," *Journal of Medical Ethics* 46/7 (2020).

21. L. Ferretti, C. Wymant, M. Kendall, et al., "Quantifying SARS-CoV-2 transmission suggests epidemic control with digital contact tracing," *Science* 368/6491 (2020).

22. Ibid.

23. N. Shah, *Contagious divides: Epidemics and race in San Francisco's Chinatown* (Berkeley: University of California Press, 2001).

24. M. Feischmidt, K. Szombati, and P. Szuhay, "Collective criminalization of the Roma in Central and Eastern Europe" in S. Body-Gendrot, M. Hough, K. Kerezsi, et al., *Routledge handbook of European criminology* (Abingdon: Routledge, 2013).

25. O. Diggelmann and M. N. Cleiss. "How the right to privacy became a human right," *Human Rights Law Review* 14/3 (2014), pp. 441–458.

26. International Covenant on Civil and Political Rights, G.A. Res. 2200A (XXI) (1966), art. 17.

27. E. M. Hafner-Burton, L. R. Helfer, and C. J. Fariss, "Emergency and escape: Explaining derogations from human rights treaties," *International Organization* 65/4 (2011), pp. 673–707.

28. Siracusa Principles on the Limitation and Derogation Provisions in the International Covenant on Civil and Political Rights, UN Doc. E/CN.4/1985/4 (1984), part. I, para. 25.

29. Ibid., part. I, paras. 1–14.

30. World Health Organization, *International health regulations (2005)*, 3rd edition (Geneva: World Health Organization, 2005), arts. 2, 5.

31. U. Gasser, M. Ienca, J. Scheibner, et al., "Digital tools against COVID-19: Taxonomy, ethical challenges and navigation aid," *Lancet Digital Health* 2/8 (2020), pp. e425–e434.

32. "Show evidence that apps for COVID-19 contact-tracing are secure and effective," editorial, *Nature* 580 (April 30, 2020), p. 563.

33. R. A. Calvo, S. Deterding, and R. M. Ryan, "Health surveillance during COVID-19 pandemic," *BMJ* 369 (2020).

34. A. Hern, "Public Health England will keep personal data of people with coronavirus for 20 years," *Guardian* (May 28, 2020). Available at https://www.theguardian.com/world/2020/may/28/nhs-will-keep-personal-data-of-people-with-coronavirus-for-20-years--uk-test-and-trace-programme.

35. T. Sharma and M. Bashir, "Use of apps in the COVID-19 response and the loss of privacy protection," *Nature Medicine* 26 (2020), pp. 1165–1167.

36. A. Sternlicht, "With new COVID-19 outbreak linked to gay man, homophobia on rise in South Korea," *Forbes* (May 12m 2020). Available at https://www.forbes.com/sites/alexandrasternlicht/2020/05/12/with-new-covid-19-outbreak-linked-to-gay-man-homophobia-on-rise-in-south-korea/#469b0b684909.

37. Public Health England, *Disparities in the risk and outcomes of COVID-19* (London: Public Health England, 2020); Sara L. M. Davis, "The uncounted: Politics of data and visibility in global health," *International Journal of Human Rights* 21/8 (2017), pp. 1155–1156.

38. S. Phartiyal, "India orders coronavirus tracing app for all workers," *Reuters* (May 2, 2020). Available at https://www.reuters.com/article/us-health-coronavirus-india-app-idUSKBN22E07K.

39. Privacy International, *Singapore contact tracing app made mandatory for migrant workers* (2020). Available at https://privacyinternational.org/examples/3890/singapore-contact-tracing-app-made-mandatory-migrant-workers.

40. International Telecommunication Union, *Measuring digital development: Facts and figures 2019* (Geneva: International Telecommunication Union, 2019).

41. J. Vitak and M. Zimmer, "More than just privacy: Using contextual integrity to evaluate the long-term risks from COVID-19 surveillance technologies," *Social Media + Society* 6/3 (2020).

42. Privacy International, *Hangzhou considers expansion options for coronavirus surveillance app* (May 26, 2020). Available at https://privacyinternational.org/examples/3888/hangzhou-considers-expansion-options-coronavirus-surveillance-app.

43. Ibid.

44. Privacy International, *Knesset committee denies exten-*

sion to police access to mobile phone location data (April 22, 2020). Available at https://privacyinternational.org/examples/3770/knesset-committee-denies-extension-police-access-mobile-phone-location-data; Privacy International, *Kenya tracks mobile phones for quarantine enforcement* (April 9, 2020). Available at https://privacyinternational.org/examples/3662/kenya-tracks-mobile-phones-quarantine-enforcement; Privacy International, *Mexican telcos grant government access to cell phone antennas* (March 31, 2020). Available at https://privacyinternational.org/examples/3691/mexican-telcos-grant-government-access-cell-phone-antennas; "Turkey to use mobile data to track isolation," *Hurriyet Daily News* (April 9, 2020). Available at https://www.hurriyetdailynews.com/turkey-to-use-mobile-data-to-track-isolation-153698.

45. Privacy International, *Pakistan repurposes anti-terrorist system for tracing COVID-19 cases* (April 24, 2020). Available at https://www.privacyinternational.org/examples/3784/pakistan-repurposes-anti-terrorist-system-tracing-covid-19-cases.

46. O. Gross and F. Ní Aoláin, *Law in times of crisis: Emergency powers in theory and practice* (Cambridge: Cambridge University Press, 2006), pp. 247–325, pp. 365–421.

47. International Covenant on Economic, Social and Cultural Rights, G.A. Res. 2200A (XXI) (1966), arts. 1, 12.

48. Universal Declaration of Human Rights, G.A. Res. 217A (III) (1948), art. 12; International Covenant on Civil and Political Rights, G.A. Res. 2200A (XXI) (1966), art. 17.

49. European Convention on Human Rights, European Treaty Series No. 5 (1950), art. 8.

50. See European Court of Human Rights, *Satakunnan v. Finland*, 931/13 (June 27, 2017).

51. European Parliament, *LIBE Committee Inquiry on Electronic Mass Surveillance of EU Citizens, Statement by Professor Martin Scheinin* (October 14, 2013). Available at https://www.europarl.europa.eu/document/activities/cont/201310/20131017ATT72929/20131017ATT72929EN.pdf.

52. *Satakunnan v. Finland* (see note 50).

53. Siracusa Principles (see note 28).

54. European Convention on Human Rights, European Treaty Series No. 5 (1950), arts. 8–11; International Covenant on Civil and Political Rights, G.A. Res. 2200A (XXI) (1966), arts. 12, 17, 18, 21, 22.

55. Human Rights Committee, General Comment No. 16: Article 17 (Right to Privacy) (1988).

56. F. Bustro and C. F. J. Doebbler, "The rights-based approach to health," in L. O. Gostin and B. M. Meier, *Foundations of global health and human rights* (New York: Oxford, 2020).

57. S. Deb, "Public policy imperatives for contact tracing in India," IFF Working Paper No. 3/2020. Available at https://docs.google.com/document/d/1nDoPzygQyTetEguOlzula5O9y5f3f5YJDsA2Pd99O6U/edit.

58. N. Bandel, "Israel's top court: No Shin Bet tracking of coronavirus patients without Knesset oversight," *Haaretz* (March 19, 2020). Available at https://www.haaretz.com/israel-news/.premium-israel-s-top-court-no-shin-bet-tracking-of-coronavirus-patients-without-knesset-ove-1.8690253.

59. Siracusa Principles (see note 28), part I, para. 10(b).

60. World Health Organization, *Surveillance strategies for COVID-19 human infection: Interim guidance* (May 10, 2020), p. 1. Available at https://apps.who.int/iris/handle/10665/332051.

61. Budd et al. (see note 13).

62. Parker et al. (see note 20).

63. Gasser et al. (see note 31).

64. UN General Assembly, Res. 68/167, UN Doc. A/RES/68/167 (2014).

65. European Court of Human Rights, *Zakharov v. Russia* 47143/06 (December 4, 2015).

66. Gasser et al. (see note 31).

67. Budd et al. (see note 13).

68. European Commission, *Coronavirus: Commission adopts recommendation to support exit strategies through mobile data and apps* (April 8, 2020) Available at https://ec.europa.eu/commission/presscorner/detail/en/IP_20_626.

69. Privacy International, *Taiwan operates comprehensive quarantine surveillance* (March 24, 2020). Available at https://www.privacyinternational.org/examples/3727/taiwan-operates-comprehensive-quarantine-surveillance.

70. G. Cohen, L. O. Gostin, and D. J. Weitzner, "Digital smartphone tracking for COVID-19: Public health and civil liberties in tension," *JAMA* 323/23 (2020), pp. 2371–2372.

71. Apple, *Apple and Google partner on COVID-19 contact tracing technology* (April 10, 2020). Available at https://www.apple.com/newsroom/2020/04/apple-and-google-partner-on-covid-19-contact-tracing-technology.

72. Budd et al. (see note 13).

73. M. Zastrow, "South Korea is reporting intimate details of COVID-19 cases: Has it helped?" *Nature* (March 18, 2020). Available at https://doi.org/10.1038/d41586-020-00740-y.

74. Privacy International, *North Macedonia launches Bluetooth-based contact tracing app* (April 16, 2020). Available at https://www.privacyinternational.org/examples/3690/north-macedonia-launches-bluetooth-based-contact-tracing-app; Australian Government, *Covidsafe privacy policy* (2020). Available at https://covidsafe.gov.au/privacy-policy.html.

75. L. Silver, "Smartphone ownership is growing rapidly around the world, but not always equally," *Pew Research Center* (February 5, 2020). Available at https://www.pewresearch.org/global/2019/02/05/smartphone-ownership-is-growing-rapidly-around-the-world-but-not-always-equally.

76. Immuni, *FAQ* (2020). Available at https://www.immuni.italia.it/faq.html.

77. T. Mrva, "Court suspends part of Slovakia's phone-tracking law to fight virus spread," *Reuters* (May 13, 2020). Available at https://in.reuters.com/article/health-coronavirus-slovakia-tracking-idINKBN22P2E3.

78. S. Sekalala, H. Masud, and R. T. Bosco, "Human

rights mechanisms for anti-corruption, transparency and accountability: Enabling the right to health," *Global Health Action* 13 (2020).

79. D. Kinley and J. Tadaki, "From talk to walk: The emergence of HR responsibilities for corporations at international law," *Virginia Journal of International Law* 44/4 (2004), pp. 931, 935.

80. D. Orentlicher and T. Gelatt, "Public law, private actors: The impact of human rights on business investors in China Symposium: Doing business in China," *Northwestern Journal of International Law and Business* 14/1 (1993), pp. 66–68.

81. Office of the United Nations High Commissioner for Human Rights, *Guiding principles on business and human rights* (Geneva: United Nations, 2011).

82. Ibid., para. 24.

83. Ibid., paras. 55–56.

84. J. Harrison and S. Sekalala, "Addressing the compliance gap? UN initiatives to benchmark the human rights performance of states and corporations," *Review of International Studies* 41 (2015), pp. 925–927.