Privacy and the pandemic: An African response

AUTHOR: Gabriella Razzano

INTRODUCTION

COVID-19 has led to a surge of efforts by both state and private actors to manage the pandemic itself, and the consequences of it, with the aid of technology. Yet privacy has immediately been cast as a required trade-off in the efforts to combat the disease. Key examples of this are being seen in the introduction of contact tracing and related surveillance interventions, worldwide. These technologies are underpinned by the personal data of citizens. The jurisprudential tools that arise from human rights discourse (such as limitations tests) provide a powerful tool for ensuring human-centred concerns are forwarded within rapidly emerging contexts, and give a particular focus for interpreting the African experience. Looking to South Africa as an example, human rights frameworks will be used to demonstrate how both privacy and access to information can serve to provide the nuance needed in assessing contact tracing, locally.

BACKGROUND

From the early stages of the global pandemic, human rights activists have tracked contact tracing and related initiatives with the objective of monitoring for potential, and exacted, human rights abuses.[1] Digitalisation in response to disasters has of course in recent years increased substantially; this extends from big data and its analysis, to the use of technology to refine and improve processes such as contact tracing.[2]

1 Privacy International. (2020). Tracking the Global Response to COVID-19. https://privacyinternational.org/examples/tracking-global-response-covid-19

2 McDonald, S. (2016). *Ebola: A Big Data Disaster.* Centre for Internet and Society. https://cis-india.org/papers/ebola-a-big-data-disaster

Contact tracing is being promoted for the fight against COVID-19 for specific reasons. Vaccines will take significant time to develop and, until a vaccine is *widely* available, the only "available infection prevention approaches are case isolation, contact tracing and quarantine, physical distancing, decontamination, and hygiene measures."[3] This is why technological solutions to contact tracing have been given such high priority.

A quantitative epidemiological study noted that, given the infectiousness of SARS-CoV-2, and with the sample data demonstrating the high level of transmission by *pre-symptomatic* patients, manual contact tracing is not sufficiently fast enough, and thus automated contact tracing should be preferred.[4] Yet, there are places that have been successful in combatting the disease without a focus on technology and with low costs. The state of Kerala in India and Vietnam, both of which also have pre-existing strong public health care systems, combatted COVID-19 successfully with a strong focus on primary health care.[5]

CONTACT TRACING TECHNOLOGIES

Often the discussions on human rights are obfuscated by the inclusion of technology – which is why attention should be paid to differentiating the types of technologies, and the purposes to which they are employed. Contact tracing focuses on tracking down those who have been exposed to a patient with COVID-19 as a method of prioritising testing and tracking the spread of the disease, which can be done both manually and/or aided by technology.[6]

States were the first to promote mobile applications with centralised data options for contact tracing. The Singapore government launched a voluntary application called TraceTogether, but it had an uptake of only 20% within the population.[7] That failure is significant, because the same study which advocated for automated contact tracing also noted that for such systems to have any efficacy, they would have to be adopted by a minimum of 65% of the relevant population.[8] Members of the public mainly stated a fear of state surveillance as being the reason for failing to download the application.[9] South Korea was

3 Ferretti, L., et al. (2020). Quantifying SARS-CoV-2 transmission suggests epidemic control with digital contact tracing. *Science, 368*(6491). https://doi.org/10.1126/science.abb6936

4 Ibid.

5 The Economist. (2020, 9 May). Vietnam and the Indian state of Kerala curbed covid-19 on the cheap. https://www.economist.com/asia/2020/05/09/vietnam-and-the-indian-state-of-kerala-curbed-covid-19-on-the-cheap

6 van Dyk, J. (2020, 26 March). Can you pause a pandemic? Inside the race to stop the spread of COVID-19 in South Africa. *Bhekisisa*. https://bhekisisa.org/features/2020-03-26-can-you-pause-a-pandemic-inside-the-race-to-stop-the-spread-of-covid19-in-south-africa

7 Criddle, C., & Kelion, L. (2020, 7 May). Coronavirus contact-tracing: World split between two types of app. *BBC*. https://www.bbc.com/news/technology-52355028

8 Ferretti, L., et al. (2020).Op. cit.

9 Sim, D., & Lim, K. (2020, 18 May). Coronavirus: why aren't Singapore residents using the TraceTogether contact-tracing app? *South China Morning Post*. https://www.scmp.com/week-asia/people/article/3084903/coronavirus-why-arent-singapore-residents-using-tracetogether

famously more successful in collecting mobile data centrally for contact tracing, but also had surveillance technologies directly in use.

Privacy concerns abound in solutions that centralise data at one point due to vulnerability and accountability. In terms of efficacy too, the reliance by African states on mobile technologies that require internet access presents a serious inhibition to efficacy where smartphone prevalence is not universal, and where data costs are prohibitive to constant online presence.[10] And there are other digital inequality risks: geolocation data from cellphone towers is less accurate in rural areas.[11] Particularly in the context of mobile phone data, there are ways to gain access to that data without a mobile application. States might approach telecommunication service providers directly for the data they hold on clients, which include geolocation points and call detail records.[12]

An alternative mobile phone solution, significantly driven by the private sector, are "peer-to-peer" solutions with decentralised data that focus strongly on Bluetooth. In such solutions, the data stays on a person's mobile device. Google and Apple collaborated to develop a shared contact tracing application programming interface (API), which means applications can be developed and made available to people through their mobile app stores. However, their protocols require the application developed to be decentralised, i.e. holding the data on the phone.[13] Many governments are seeking to amend their solutions to comply with this protocol (as availability through the store could improve voluntary uptake by citizens), though there are concerns that the designs may not adapt well.[14] This decentralisation is meant as a nod to privacy, though commentators have noted that the device manufacturers themselves do not have perfect privacy track records.[15]

HUMAN RIGHTS AND CONTACT TRACING

HUMAN RIGHTS LIMITATIONS

The principles of legality and proportionality have long had reference in international human rights law for understanding justifiable limitations of rights.

10 Gillwald, A., & Mothobi, O. (2019). *After Access 2018: A demand-side view of mobile Internet from 10 African countries*. Research ICT Africa. https://www.africaportal.org/documents/19044/2019_After-Access_Africa-Comparative-report.pdf

11 McDonald, S. (2016). Op. cit.

12 Oliver, N., et al. (2020). Mobile phone data and COVID-19: Missing an opportunity? *ArXiv:2003.12347*. https://arxiv.org/abs/2003.12347

13 Criddle, C., & Kelion, L. (2020, 7 May). Op. cit.

14 Ibid.

15 Kaye, D. (2020). *Disease pandemics and the freedom of opinion and expression: Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression.* http://daccess-ods.un.org/access.nsf/Get?Open&DS=A/HRC/44/49&Lang=E; Mansell, R. (2020, 23 April). Coronavirus contact tracing apps – a proportionate response? *Media@LSE*. https://blogs.lse.ac.uk/medialse/2020/04/23/coronavirus-contact-tracing-apps-a-proportionate-response

Proportionality has been interpreted to include necessity and reasonableness,[16] though often it is referred to as a separate test for limitations.[17] These tests help challenge a false dichotomy that arises in much commentary, which pits privacy as competing against public health, and thus public health requiring "privacy trade-offs".[18] Human rights principles are designed specifically to consider the balance between "competing" interests, and a recognition that rights (whether to health or privacy) are not absolute.

These principles have already been used to assess specific contact tracing initiatives worldwide.[19] France's data protection watchdog, in considering the introduction of a voluntary contact tracing application called "StopCovid", considered many aspects of the application to be problematic. In particular, it held that "the invasion of privacy will be admissible in the present case only if [...] the Government can rely on sufficient evidence to have reasonable assurance that such a measure will be useful in managing the crisis."[20]

In other words, it considered the reasonableness, while also considering whether the measures were proportional to their intended purpose. Vitally, too, it highlights the importance of evidence (and sufficiency of evidence) for an inquiry into necessity.[21] The Israeli Supreme Court held that its version of contact tracing was not properly authorised by law.[22] While it doesn't appear as if there has been any direct litigation on contact tracing technologies in Africa, in a recent South African judgement, *Amabhungane Centre for Investigative Journalism NPC and Another v Minister of Justice and Correctional Services and Others* [2019] ZAGPPHC 384, it was held that mass surveillance being performed in the country was unconstitutional because of the lack of express empowering legislation to do.

THE RIGHT TO PRIVACY

The right to privacy is at the forefront of conversations on contact tracing. In Africa, personal privacy was not prioritised previously as a rights area given

16 Cianciardo, J. (2009). The Principle of Proportionality: Its Dimensions and Limits. *ExpressO*. https://works.bepress.com/juan_cianciardo/1

17 Mansell, R. (2020, 23 April). Op. cit.

18 Servick, K. (2020, 22 March). Cellphone tracking could help stem the spread of coronavirus. Is privacy the price? *AAAS*. https://www.sciencemag.org/news/2020/03/cellphone-tracking-could-help-stem-spread-coronavirus-privacy-price

19 Renieris, E. M. (2020, 18 May). The Dangers of Blockchain-Enabled "Immunity Passports" for COVID-19. Medium. https://medium.com/berkman-klein-center/the-dangers-of-blockchain-enabled-immunity-passports-for-covid-19-5ff84cacb290

20 CNIL. (2020). Deliberation N°. 2020-046 of April 24, 2020 delivering an opinion on a proposed mobile application called "StopCovid". https://www.cnil.fr/sites/default/files/atoms/files/deliberation_of_april_24_2020_delivering_an_opinion_on_a_proposed_mobile_application_called_stopcovid.pdf

21 Renieris, E. M. (2020, 18 May). Op. cit.

22 Or-Hof, D., & Perelman-Farhi, R. (2020, 1 May). Striking the right balance: Government contact tracing powers and the right to privacy. *IAPP*. https://iapp.org/news/a/striking-the-right-balance-government-contact-tracing-powers-and-the-right-to-privacy

its association to individualised, rather than communal, rights.[23] However, the African Commission on Human and Peoples' Rights (ACHPR) has published a revised Declaration on Principles of Freedom of Expression and Access to Information in Africa, 2019, which now expressly recognises the protection of personal information as an aspect of the right to privacy.

In addition, most African countries' individual constitutions directly protect privacy, though not always in relation to information. The right to privacy for information and data is often given expression through specific data protection laws.[24] Thirty-three African countries have data protection laws that could be directly applied to their country contexts.[25] Laws that limit data processing by the public and private sector help directly prevent privacy harms against citizens. The emerging international rights regimes on data protection are largely principles-based, and those principles typically include:

- Collection limitation
- Purpose specification
- Use limitation
- Data quality
- Security safeguards
- Openness
- Accountability
- Data subject rights.

Principles that consider data minimisation at collection are particularly noteworthy for contact tracing contexts, with the ACHPR Declaration specifically noting in Article 42 that data collection must be "in accordance with the purpose for which it was collected, and adequate, relevant and not excessive." Consider, too, limitations on use *and* retention: just because collecting data may be necessary for a purpose does not mean that the retention of that data can outlast its purpose. The scientific study that promoted digital contact tracing as a necessity for combatting COVID-19 itself acknowledged that such activities should only create a "temporary record".[26]

However, once data is collected, it is hard to "reverse" this process. Deletion of records needs to be strictly monitored, and anonymisation of data can be challenging – de-identification will ordinarily not be enough, with studies specific to mobile phone data showing only four data points from a call detail record could be used to re-identify a person.[27]

---

23 Boshe, P. (2017). *Data Protection Legal Reform in Africa*. Passau University.

24 Case law related to data privacy, and associated legislation, has been demonstrated in such high-profile cases as *Nubian Rights Forum & 2 others v Attorney General & 6 others; Child Welfare Society & 9 others (Interested Parties*) [2020] eKLR (Kenya) and *Madhewoo v The State of Mauritius & Another* 2015 SCJ 177 (Mauritius).

25 Greenleaf, G., & Cottier, B. (2020). 2020 ends a decade of 62 new data privacy laws. *Privacy Laws & Business International Report,* 24-26. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3572611

26 Ferretti, L., et al. (2020).Op. cit.

27 de Montjoye, Y.-A., Kendall, J., & Kerry, C. (2014). *Enabling Humanitarian Use of Mobile Phone Data*. Brookings

While the right to privacy provides obvious parameters for limiting contact tracing initiatives, so too the right to access information provides important accountability parameters. The right of access to information has been supported by strong campaigns across the African continent.[28] Article 9 (1) of the African Charter on Human and Peoples' Rights states expressly that "[e]very individual shall have the right to receive information."Public accountability for the state authorisation and implementation of contact tracing applications must correspond with the provision of sufficient information about both the system itself, and its implementation.[29] Even the algorithm that underscores the contact tracing process should be transparent, as should associated modelling.[30] Ideally, particularly given the risks associated with surveillance, oversight of the implementation of contact tracing should be judicial – and this judicial oversight needs to have sufficient access to information, too.[31]

Information is needed not just for accountability purposes, but also to support a citizen's right to make an informed decision.[32] The rights to data privacy and access to information thus support each other in the contact tracing context: high levels of public trust are required to ensure an *effective* level of uptake by citizens, and access to information forms a vital precursor for ensuring real consent. In the fight against the Ebola virus, mistrust in government information directly impeded contact tracing efforts.[33]

Provision of suitable access to information has an essential role within the public health context of COVID-19: the "goal in a public health crisis must be for government to provide accurate information."[34] Contact tracing can certainly contribute to these ambitions by assisting in creating the data and evidence base for making public health decisions, but only if supported by a fully rights-respecting design and implementation.

APPLICATION TO SOUTH AFRICA

On 15 March 2020, South Africa declared a national state of disaster, which allowed for the passing of regulations to help manage the COVID-19 pandemic. Initial regulations, scant on details about a possible contact tracing solution, were quickly amended on 2 April 2020 (Disaster Management Act, 2002:

Institute. https://www.brookings.edu/research/enabling-humanitarian-use-of-mobile-phone-data

28 See, for example, the African Platform on Access to Information: http://www.africanplatform.org

29 Mansell, R. (2020, 23 April). Op. cit.; Razzano, G. (2020, 25 May). Covid-19 – why a mysterious disease shouldn't result in mysterious decisions. *Daily Maverick*. https://www.dailymaverick.co.za/opinionista/2020-05-25-covid-19-why-a-mysterious-disease-shouldnt-result-in-mysterious-decisions

30 Ferretti, L., et al. (2020).Op. cit.; Razzano, G. (2020, 25 May). Op. cit.

31 Kaye, D. (2020). Op. cit.

32 Mansell, R. (2020, 23 April). Op. cit.

33 McDonald, S. (2016). Op. cit.

34 Kaye, D. (2020). Op. cit.

← "Privacy need not be unduly sacrificed in pandemic responses if rights-based solutions are properly explored". Source: Etienne Girardet on Unsplash

Amendment of Regulations, 2020). These regulations outlined the South African government's main solution to contact tracing as being expanded powers for the health authorities to obtain geolocation data and personal identifiers of any person who is reasonably suspected to have contracted COVID-19, or who has come into contact with someone who has COVID-19, directly from telecommunication service providers (and without a court order).[35] This information is then fed into a contact tracing database held by the Department of Health (DOH), for which the Director-General is responsible. Though no order is required to collect the data, a respected former Constitutional Court judge, Justice Kate O'Regan, was appointed as the designated COVID-19 judge to monitor the collection and use of location data for the contact database.[36] Considered in terms of privacy and data protection, the dramatic delays in enacting South Africa's Protection of Personal Information Act, 2013 (POPIA) are highly problematic. POPIA created an Information Regulator, who has been in position since December 2016. Yet the main sections of the Act have only just recently been made operational from 1 July 2020. This operationalisation gives both public and private sector data processors a full year to become fully compliant from that date. The regulations make no reference to the Information Regulator or POPIA, probably as a result of the fact that when they were passed, POPIA was not yet fully enacted.[37] This means that, at one of the most pivotal

35 Gillwald, A., Rens, A., van der Spuy, A., & Razzano, G. (2020, 27 April). Mobile phone data is useful in coronavirus battle. But are people protected enough? *The Conversation*. https://theconversation.com/mobile-phone-data-is-useful-in-coronavirus-battle-but-are-people-protected-enough-136404

36 Ibid.

37 Ibid.

moments in South Africa's data privacy history, the only office with the requisite insight and powers – and in the South African case, a dual mandate between access to information and privacy – is excluded from the implementation and accountability processes.

Nevertheless, data protection principles provide a useful frame for understanding the regulations. There is purpose limitation: data may only be collected, used and disclosed by authorised persons for the purposes of addressing, preventing or combatting the spread of COVID-19 through the contact tracing process for the tracing database.

There is also at least allusion to keeping the data secure: the regulations require the information to be kept "confidential". Unlike other countries which have centralised the data with security agencies, thus increasing concerns of abuse of data for surveillance purposes, the database vests with the DOH.[38] However, the agency itself does not have an impervious data protection record.[39] This highlights the need for effective accountability, and this is where key challenges emerge. While the Director-General provides weekly reports to the designated judge, this doesn't automatically provide her with direct access to the database – the key information necessary for properly informing oversight.[40]

The duration of the lawful data retention terminates with the end of the national state of disaster, though de-identified data will be retained. The ability of the state to effectively and authentically de-identify thus becomes of immense concern.[41] Sufficient access to information has to be provided not just to the overseeing judge, but in terms of records management to ensure purpose specification was complied with.[42] This is aided by the partial nod provided to direct data subject rights by the regulations, which require that every person whose information was obtained be notified of such within six weeks of the national state of disaster lapsing. It is not clear, however, why the regulations do not require alerting data subjects simultaneously as the data is collected, particularly as the purpose is for contact tracing rather than surveillance.

Data opportunism is always a concern in a large-scale data collection exercise. In terms of the abuse of this data for surveillance, real questions will concern that defined purpose: can we be assured the data will not be handed over to the security agencies for monitoring quarantine surveillance, for instance? Again, this is why accountability and access to information must be prioritised in both the drafting of the regulations, but also in the practice of their implementation.[43] Privacy implications are best understood in the context of both the technology concerned

38 Wild, S. (2020, 12 May). Antipoaching Tech Tracks COVID-19 Flare-Ups in South Africa. *Scientific American*. https://www.scientificamerican.com/article/antipoaching-tech-tracks-covid-19-flare-ups-in-south-africa

39 Bateman, B. (2019, 11 March). Exclusive: National Health Lab Services is sharing patient records. *EWN*. https://ewn.co.za/2019/03/11/exclusive-national-health-lab-services-accused-of-unlawfully-sharing-patient-records

40 Gillwald, A., Rens, A., van der Spuy, A., & Razzano, G. (2020, 27 April). Op. cit.

41 de Montjoye, Y.-A., Kendall, J., & Kerry, C. (2014). Op. cit.

42 Kaye, D. (2020). Op. cit.

43 Ibid.

and the implementation reality.[44] The South African state is not seeking, currently, to institute a mobile application. Instead, the contact tracing database seeks to support manual tracing exercises, which currently rely on 60,000 health care workers who go door to door asking for symptoms.[45] In addition, primary health care workers and responders manually collate contact tracing details from patients that test positive, and businesses are beginning to collate contact tracing details as lockdown lifts. It is therefore important to remember that it is not the use of technology itself which threatens privacy – it is the nature of personal data, with the technology amplifying some of the risks. There has already been the report of a woman in the United States being stalked by an employee of a business to which she was required to hand over her personal data, without technology interceding.[46]

That broader data protection principles are not currently fully enforceable in a country where the mass collection of data is being actively driven by the state is a serious concern. While the regulations commit to limiting the retention of the data, it is worth noting that in the past, serious questions have been raised about the efficacy of the South African government's disease surveillance in practice – highlighting questions on the efficacy of the programme being instituted.[47] The proportionality and necessity of the government's response will become clearer with implementation, and with due consideration to both access to information and privacy.

CONCLUSION

Human rights provide an essential frame for considering contact tracing initiatives in the African context. Privacy, a right of increasing relevance in African human rights jurisprudence, need not be sacrificed for an effective fight against COVID-19. Instead, ensuring the interventions promote access to information, privacy and other rights should be a priority for contact tracing implementers to ensure public trust (and uptake). As one commentator noted: "You manage an epidemic by being more open, more democratic and allowing for critical review and comment."[48] When technology is considered outside of context, techno-centrism threatens to steamroll rights. This is especially because of the increasing reliance of such technologies on big (and personal) data. Yet considering proportionality and necessity, this techno-centrism itself – given digital inequalities – threatens the justifications for many contact tracing initiatives in our country contexts. Civil society actors seeking to assess contact tracing

44 Nissenbaum, H. (2009). *Privacy in Context*. Stanford University Press.

45 van Dyk, J. (2020, 26 March). Op. cit.

46 Vaas, L. (2020, 14 May). Woman stalked by sandwich server via her COVID-19 contact tracing info. *Naked Security*. https://nakedsecurity.sophos.com/2020/05/14/woman-stalked-by-sandwich-server-via-her-covid-19-contact-tracing-info

47 Benson, F. G., Musekiwa, A., Blumberg, L., & Rispel, L. C. (2016). Survey of the perceptions of key stakeholders on the attributes of the South African Notifiable Diseases Surveillance System. *BMC Public Health, 16*, 1120. https://doi.org/10.1186/s12889-016-3781-7

48 Wild, S. (2020, 12 May). Op. cit.

initiatives being proposed domestically should be guided first by defining technologies proposed in detail, as well as the intersections explored in this paper, to consider the real privacy risks in context.

Emerging African jurisprudence on privacy has focused strongly on legality and lawfulness. This lends support to activism to promote the adoption of principles-based data protection legal regimes. Importantly, too, as emerges from the examples considered, these data protection regimes must be complied with by both the state and private actors, as both have mass data collection incentives.

The South African case study in particular raises a very specific recommendation for the promotion of new contact tracing intervention: the role of data protection authorities should be prioritised. To not do so, is to fail to place these emergency responses within the strong controls that are beginning to emerge on personal privacy protection.