Tech-mediated Tracking: A Viable Tool to Contain COVID-19 in Ethiopia?

By:

Kebene Wodajo
Dawit Ayana

June 2, 2020

The dire situation caused by COVID-19 has led governments to explore options for various alternatives to control its spread. Alongside other measures, states across the globe, including some African nations, are introducing contact-tracing through mobile/smartphone apps. This is particularly so in South Korea, Taiwan, China and Singapore East and Southeast Asian countries. Europe and the US are also considering the alternative. The effort is gaining further ground with updates coming from large tech companies like Apple and Google – collaborating to provide a software application programming interface (API). The interface enables to let authorised COVID-19 contact-tracing apps to work effectively and securely by using Bluetooth technology. The contact-tracing app will be developed by the public health authorities of countries. Likewise, Europe is sorting alternatives – through 'Pan-European Privacy-Preserving Proximity

Tracing' (PEPP-PT), which is working on tracing app that will use Bluetooth and other technologies. This is more or less similar to that of Singapore's Trace Together app, which uses Bluetooth and location services to trace. AI and big data are also deployed by countries like China. China is using facial recognition technology and 'smart' thermal scanners in public spaces to track the spread of the virus.

Following these trends, Ethiopia's Information Network Security Agency (INSA) also developed a Covid-19 monitoring app that would help to trace people's contact through voluntary subscription. The subscription would help to locate with whom the person came in contact. Detail is not available on the data privacy of people. Other Sub Saharan African (SSA) countries, including Kenya, South Africa, Uganda, and Ghana, are also considering to implement mobile technology-based surveillance.

Living at the age of surveillance capitalism where social life is datafied and data is abused and exploited, it is necessary to probe these efforts further before they are implemented. In our view, surveillance through tech-mediated tracking might help with contact-tracing, but at what cost?

In situations of health crises, it is necessary and intuitively right to put technology as one of the responses. However, it is equally important to scrutinize and carefully establish the intended and unintended consequences of such measures. Our brief reflection focuses on how technology-mediated tracing means for data privacy in SSA, particularly Ethiopia.

Risks and Opportunities

There are both opportunities and risks in deploying surveillance as a tool for the containment of COVID-19. That said, it is essential to keep in mind that the efficacy and correlation of surveillance to reduce the spread of the virus is debatable. Diagnostic capacity and how well organized the testing system is together with societal culture play a significant role. Therefore attempts to use surveillance must be conscious of the opportunities and risks that may arise during and post COVID-19 crises. Below are some of these pros and cons:

Opportunities Given the nature of digital space, mobile tracing may relatively look efficient and less costly. It certainly is preferable than a pen and paper log in terms of reducing error and saving time. Optimism in tech redemptive power induces many, including high league entities such as the University of Oxford team to come out with "IT IS POSSIBLE TO STOP THE EPIDEMIC". Yes, it would be possible, but the how, where, when, and who questions matter most. Success in using this digital tool is conditional on various factors. Among others, the basic ones include – internet and/or mobile data penetration, smartphone distribution, and literacy rate (both digital and non-digital literacy). The limited availability and distribution of internet and mobile phones means that it would be wishful to think of surveillance as a viable alternative to contain the spread of the virus. A step further, unless the people with access to these tools have the necessary level of literacy that would enable them to use the digital platform, it is again of minimum help. Unsurprisingly, all these factors significantly impact the efficacy of the surveillance alternative in SSA. Excluding the Southern African sub-region, the proportion of internet penetration and mobile connectivity in all the other sub-regions of SSA are the lowest in the world. They also share the lowest proportion of mobile internet subscribers globally. In the particular case of Ethiopia, mobile connectivity and internet penetration are 41 % and 19 %, respectively. Further, the county's adult literacy rate is 52 %. With this weak infrastructure, it is highly questionable to what extent the surveillance option would help Ethiopia and the majority of the SSA to contain the virus effectively.

Risks The risk of deploying digital tracing to control the spread of the virus can be split into two – during/in the process and post COVID-19 crisis. The first risk is in the process of battling the pandemic. At this stage, the surveillance tool may enable expansive social surveillance and rights violations. This concern has been raised by different stakeholders and rights defenders. This raises the question about how to balance the rights to health and life against the right to privacy. International human rights instruments oblige governments to protect, respect, and remedy fundamental rights such as the right to life, health, and privacy. Nevertheless, in times like now, governments may have to temporarily restrict some human rights to respond to health emergencies in a proportional, timely, and coordinated way. That said, unless governments' and tech companies' role throughout the process is kept in check, there are risks to.

Such risks are notably higher in countries with repressive regimes where state surveillance is a norm and legal infrastructure is weak.

In this regard, SSA, except for a very few countries especially Ethiopia, do not have a good record of internet freedom. A 2019 internet freedom index by the Freedom House shows that only South Africa and Kenya have the highest index rankings with 72 and 68 out of 100, respectively. Other SSA countries having a lower index, Ethiopia, 28 and Sudan, 25 being the least free countries in the region. Given this fact, the risk of surveillance deployment for pandemic control in the region and Ethiopia, in particular, is even higher.

The other risk is the diversion of resources from a rather efficient and effective containment alternative. As mentioned, the efficacy and correlation of phone tracking in controlling the spread of COVID-19 is still unsettled. Added to that, in areas where the necessary infrastructure such as sufficient internet and mobile connectivity is scant, its efficacy is questionable. Hence, governments may end up spending resources inefficiently. That is the expense they incur to deploy such technology that would have been used on relatively better alternatives.

The third risk of automated tracking is its potential to become a permanent fixture after the end of the pandemic. Mobile tracking deployed for coronavirus purposes may continue as a 'new normal'. If history teaches us anything, it us that surveillance measures adopted after the attacks against the United States in September 2001 stayed in force long after on the pretext that they were necessary in the war against terrorism.

Keeping the right balance

Yuval Noah Harari argues that the underlying problem is asking citizens to make a trade-off between health and privacy. The right way to deploy to combat COVID-19 is in a manner that empowers citizens. For example, Microsoft's seven principles can help preserve privacy while addressing COVID-19. These are – measures taken must be lawful, follow the due process, necessity, proportionality, transparency, time-bound, and run under well-organized oversight. The use of phone tracking is lawful and follows due

process when peoples' data is obtained through meaningful and informed consent of users. It is necessary and proportional when the data collected is only for public health purposes, and the amount is kept at a minimal amount. It is transparent when users are provided with and informed about a choice whether their data is stored, where it would be stored, how secure it would be, and whether or not is shared with their consent. Time-boundedness means that the data shall be deleted as soon as the crisis or emergency are over.

Takeaway for Ethiopia

Against the preceding discussion, we believe that the attempt to deploy tracking technology in Ethiopia seems to pose risks than opportunities. Hence, it merits critical reflection. The following are a few points we set forward as a conversation starter.

First, the detail on how the application works and the extent of data to be collected is not transparent. On a related note, the location where the data collected will be stored and how secure it would be is not known. Therefore, it lacks clarity at many levels. Second, as the above shown data suggest, the internet penetration, mobile connectivity, and literacy rate in Ethiopia strongly shatter the efficacy of the technology to control the virus. Third, this might even result in inefficient resource diversion from rather beneficial and efficient containment alternatives. Lastly, given a poor track record of Ethiopia in digital freedom and weak legal infrastructure for privacy and data protection, the risk of a permanent fixture is expected.

To end with Harari’s note, "…, the storm will pass, humankind will survive, most of us will still be alive — but we will inhabit a different world." Our question then – would that world be one we live under expansive surveillance or where the right balance is kept? We believe that it depends on the ethics and commitment of both governments and tech companies to comply with and aspire to empower citizens through technology than datafication and then commodification of social life.

View online: Tech-mediated Tracking: A Viable Tool to Contain COVID-19 in Ethiopia?

Provided by Afronomicslaw