Title: Digital Surveillance Systems to Combat COVID-19 May Do More Harm Than Good

Author(s): Kritika Bhardwaj


ISSN (Online): 2349-8846

Published by: Economic and Political Weekly (Engage)

Article URL: https://www.epw.in/engage/article/digital-surveillance-systems-combat-covid-19-harm

Author(s) Affiliation: Kritika Bhardwaj (kritika.bhardwaj12@gmail.com) is an advocate and a fellow with the Centre for Communication Governance at the National Law University, Delhi.

Articles published in EPW Engage are web exclusive.
Digital Surveillance Systems to Combat COVID-19 May Do More Harm Than Good

Kritika Bhardwaj

Abstract: A pandemic admittedly requires the extensive gathering of data and surveillance to understand disease trends, infrastructural constraints, and to frame prevention and mitigation strategies. However, the objective of securing public health, crucial as it may be, cannot be oblivious to constitutionally-guaranteed civil liberties.

Concerns about the impact of disease surveillance on individual rights—including privacy—are not new. Globally, previous epidemics have led to an increasing acceptance that public health initiatives must also respect freedom and privacy to the greatest extent possible. However, India does not appear to have factored this into its response to the COVID-19 pandemic. Rather, what we are witnessing is a push to develop and adopt ad hoc technology-based solutions without a clear understanding of their limitations and harms. Lessons from history and other jurisdictions show that a rights-friendly response to the pandemic is possible and must be strived for.^[1]

Lessons from the Past

While the scale of the present pandemic is unparalleled, concerns regarding liberty and privacy in the context of disease surveillance have arisen several times in the past. In fact, with the rise of big data tools and algorithmic decision-making, such concerns have only increased in recent years. The 2003 severe acute respiratory syndrome (SARS) outbreak spurred an active debate in Canada on the need to balance individual liberty while simultaneously tackling infectious
diseases. In response, Canada amended its Quarantine Act in 2005 to give legislative basis to excessive powers that the state may exercise in the event of a disease outbreak, and also placed limits on these powers. These include the right to challenge a quarantine order, the obligation to seek consent or a warrant to inspect a dwelling place, and to give notice to an individual whose personal information is shared by the government in order to prevent the spread of the infection.

Similarly, in 2015, South Korea also amended the Infectious Diseases Control and Prevention Act, 2009 to control the spread of a disease after the country faced the Middle East respiratory syndrome (MERS) outbreak. While conferring wide powers upon the government to collect personal information, the law imposes a similar obligation to notify persons if and when their information is collected as well as an obligation to delete data when it is no longer necessary to secure public health.

In 2017, the World Health Organization (WHO) published its guidelines on "Ethical Issues in Public Health Surveillance" (WHO 2017). These guidelines require states to ensure that there is no unauthorised access or disclosure of information collected and requires them to take stock of how much data is rightfully required by various agencies of the government before access is granted. For example, granular personal data may be required at the local level, but higher levels of government only require aggregated anonymised information. Similarly, to preserve public trust in the surveillance system, the WHO guidelines warn against using personal data for non-public health uses.

The Indian Regime for Disease Surveillance and Digital Solutionism

A scrutiny of the measures adopted by the Indian government reveals that its response to the pandemic has been ad hoc, reactionary, and wholly outside the framework of any public health legislation. This has resulted in the rise of misconceived digital “solutions” without any consideration of how they may impact civil liberties.

The absence of a well-defined legal regime for public health is problematic for several reasons. During an epidemic (or in this case, a pandemic), state agencies may act in a way that significantly impacts people’s fundamental rights to liberty, free movement, and privacy. Authorities may have to compel individuals to undergo testing, mandatory isolation and/or enforce quarantine measures, and trace all of their interactions in case they test positive for the infection. With such grave implications for civil liberties, a legal framework is essential to bring certainty and accountability to government functioning. It will have checks and balances in place and will state the rights and remedies of those affected by the wrongful exercise of powers.
In India, the National Centre for Disease Control, constituted under the Ministry of Health and Family Welfare, is tasked with disease surveillance and the institution of containment measures. In a 2015 report on India’s compliance with the WHO’s International Health Regulations—currently the only global regulations on public health, which are binding on India—the WHO observed the absence of appropriate legislation that would enable the Indian government to mobilise its different wings in the case of an imminent outbreak (WHO 2015). The report noted that this legal gap is exacerbated when coordination is required with states, presumably because health is a domain over which states have exclusive powers. The report also noted that India lacks a standard operating procedure (SOP) to clarify when existing legislative provisions could be invoked, and who could be directed to respond to the outbreak. However, in nearly five years since this report was published, there is still no sign of a legal regime to describe the powers of the state and its functions during such times.

In the absence of such an SOP, states in India have resorted to invoking the Epidemic Diseases Act, 1897—a pre-independence legislation that confers extremely wide powers on states without any procedural safeguards. In order to exercise powers under this statute, most states have framed regulations under it, conferring upon themselves the power to impose and enforce quarantine and to collect vast amounts of personal information. These regulations are vaguely worded and contain no limitations or safeguards. Similarly, on 24 March 2020, the central government invoked the Disaster Management Act, 2005, which allowed it to issue binding guidelines to states. The central government’s entire response to COVID-19 has been through these guidelines, including its imposition of a strict nationwide lockdown for over two months. The result has been the issuance of top-down orders, even though much of the economic and infrastructural burden has fallen directly on state governments.

Instead, a consequence of these ad hoc, play-by-ear executive guidelines has been the alarming increase in the adoption of digital technology, with the supposed objective of overcoming existing infrastructural gaps; India spends approximately 1.28% of its gross domestic product on health (Chandna 2019). Such technologies are often rolled out with neither understanding their limitations, nor properly examining their potential to harm (Kak and Joshi 2020). More worryingly, an over-reliance on technology also makes the state complacent; technological interventions tend to become the default, replacing efforts to understand and address the underlying causes of the problem (Morozov 2020).

The most notable of such digital interventions has been the creation of Aarogya Setu, a contact-tracing application being used to identify who a user interacted with in order to warn them in case the user tests positive for the infection. States have also taken to widespread deployment of drones in several cities to enforce quarantine measures as well as the lockdown itself.

More recently, Broadcasts Engineering Consultants India Limited (BECIL), a public sector
undertaking, issued expressions of interest to invite bids for a "personnel tracking GPS solution" as well as a "COVID-19 patient tracking tool (BECIL 2020a, 2020b)." The first envisages a wearable device to track health workers’ location and to store the data on a centralised government server. The second proposes the collation of information from government databases and from telecom and internet data to identify “locations, associations and behaviour” of patients/persons suspected of being infected.

However, evidence suggests that these interventions may only end up ramping up surveillance without achieving any of their stated objectives.

**Digital Solutions: Inherent Limitations and Surveillance Harms**

There is wide consensus that no digital contact tracing solution can replace efforts on the field. Such apps are inherently limited: first, their success depends on self-reporting by confirmed infectious persons, which in turn depends on large-scale testing. Given India’s abysmally low testing rate, self-reporting too will predictably be low. Second, in view of India’s low smartphone penetration, it is likely that the app will be ineffective for a large part of the population; third, such apps assess risk based on Bluetooth signals, which may result in false positives as the signals are capable of transmitting across walls or ceilings, therefore alerting people in adjoining houses or cars, even in the absence of physical contact. In fact, the app has already been used to forcibly send someone to a quarantine facility despite the fact the individual had not left her home for several weeks (Quint 2020).

In 2014, cell phone site location, global positioning systems, and data from call records were championed as pathbreaking tools in preventing the spread of Ebola in West Africa. However, research from Sierra Leone showed that an over-reliance on cell-phone data proved ineffective for failing to account for local realities such as a large number of people not owning cell phones, a single phone being shared by several family members, and patchy signal network coverage (Erikson 2018). With Aarogya Setu, we are likely to repeat the same mistakes rather than learn from them.

In addition to these limitations, such technological tools also vastly expand the government’s surveillance architecture, meriting a need to assess whether they are actually essential and whether any alternate, less-intrusive means exist to achieve the same ends.

Aarogya Setu, for instance, collects a large amount of personal information from users when they sign up, and constantly builds on this by collecting location and Bluetooth data in real time. This allows the app to create a social graph of a person’s interactions. Neither the app nor the Data Access and Knowledge Sharing Protocol—which was subsequently issued—provide...
for a fixed period of time after which the collected data will be destroyed (Ministry of Electronics and Information Technology 2020). The protocol also reveals that the app’s functionality is not limited to contact tracing, but that the data gathered through it will be used to inform government decision making on almost all aspects related to COVID-19. The government recently relied on the data generated by the app to identify new hotspots. But the inherent limitations of the app referred to above make these decisions highly suspect. This is in addition to some states in India promoting their own applications for contact tracing and geofencing, which raise similar concerns.

The use of hired drones by the police for surveillance also raises several concerns (Internet Freedom Foundation 2020). These drones are being deployed without any legal basis or transparency on how the recorded footage will be used or retained. A number of troubling scenarios are possible—the data may be used to surveil and target specific locations or communities that are already subjected to discrimination and harassment. It may also be retained and used later for purposes unrelated to disease surveillance. Reports suggest that this data is already being shared freely amongst various entities of the government without people’s knowledge or consent (Livemint 2020).

The BECIL tenders are even more dystopian; they aim to combine various invasive technologies like location tracking and facial recognition in order to create tools for mass surveillance without any perceived need for them.

What Does Privacy-friendly Disease Surveillance Look Like?

In 2017, the Indian Supreme Court affirmed the right to privacy as a fundamental right. The ruling laid particular emphasis on informational self-determination, which is an individual’s right to determine how information about them should be collected and used. No doubt, public health interests may require some restrictions to the right to privacy—as was expressly recognised by the court itself. However, any restriction must necessarily pursue a legitimate aim, be based in law, and be a necessary and proportionate means to achieve said aim. This means that the state must first identify the goals it seeks to achieve rather than first creating surveillance mechanisms and then continuously shifting the goalposts. If multiple ways exist to achieve an objective, the state is obliged to adopt the least restrictive one. However, the expansive and constantly evolving use of Aarogya Setu suggests that the government has clearly failed to meet these requirements.

The legal regime for public health, such as in Canada and South Korea, is therefore essential to ensure that public safety is not used as an excuse to unnecessarily restrict constitutionally guaranteed freedoms. The state needs to be transparent about the digital tools it adopts, which
would only go towards increasing public trust and ensure better adoption of the technology. Individuals should be informed if their information has been collected and used by the government for surveillance or research purposes, giving them an opportunity to challenge the government’s acts if they feel such powers are wrongly exercised.

If surveillance is legitimately warranted to deal with a public health emergency, then it must be subject to a sunset clause. Data that is no longer required must be deleted and clear protocols need to be created to determine who can access the data in case it has to be retained for research or medical purposes.

The years following the 9/11 terrorist attack in the United States (US) saw an exceptional rise in the use of surveillance technology worldwide. The attack led to prioritising security interests over all freedoms, thus facilitating the creation of unprecedented systems of mass surveillance. Instead of cracking down on the private sector for the exploitative use of personal data, intelligence agencies urgently turned to them to help develop their own systems (Zuboff 2019). The nature of the attack—and the extent of loss and suffering—led to a feeling that these were exceptional times, necessitating the widespread adoption of surveillance technology.

However, two decades later, there is near unanimous consensus that such far-reaching surveillance did little to prevent subsequent attacks.[4] Rather, these measures normalised surveillance that was introduced at an "exceptional" time. In the US, this also prevented the introduction of robust regulation to control the use of personal data, lest it hamper the government's grand security project.

Today, the rise of digital surveillance tools to combat COVID-19 is reminiscent of the situation two decades ago. However, we then had limited understanding of such digital technology at the time and could not easily articulate the harms arising from it. Today, the situation is different. Our past experiences can and should inform our resistance to the similar deployment of dystopian surveillance technology under the guise of public health.

Endnotes:


References:


