Tracking Covid-19 using big data and big tech: a digital Pandora's Box

Stephen L Roberts *explains why, despite the supplemental value of some digital surveillance practices in the tracking of disease outbreaks, the concerns which arise from their use are multi-faceted and complex.*

The Covid-19 pandemic has brought new big data-driven practices of infectious disease surveillance to the forefront of efforts to track cases in real-time. As infections have continued to spread across the globe, governments have increasingly sought to capitalise on the volume, variety and velocity of the Big Data era, and to partner with Big Tech corporations in order to accelerate the surveillance of infected populations.

China has led the global charge in harnessing the digital turn of infectious disease surveillance practices in order to monitor the movement of its citizens, to track suspected infections in real-time, and in the unprecedented quarantining of tens of millions of citizens at critical phases of the pandemic. China's employment of big data-driven tactics of population surveillance is without parallel in this pandemic: ranging from the accessing and monitoring of citizens' use of social media and communication apps, to the use of drone technology to enforce population quarantine, to the application of facial recognition technology to identify suspected infected individuals. Most recently, Hanwang Technology Co. (Hanvon), China's leading firm specialising in recognition technology, whose client-base includes the Chinese Ministry of Public Security, announced that it had developed the first facial recognition technology which made it possible to successfully identify persons even when they are wearing facemasks.

Elsewhere, states have also opted-in to the intensifying union of 'Big Data and Big Tech' with public health security measures. Taiwan, for example has sought to control its national rate of infections through implementing an 'electric fence' programme which uses mobile phone location-tracking to ensure quarantined persons remain in their home. Similar measures aimed at limiting population movements by digital mediums have also been implemented in Singapore. The Russian government has also intensified its digital surveillance activities by operationalising thousands of security cameras in urban centres enabled with facial recognition technology. In recent weeks, Israel announced it would be commencing the tracking of mobile phones to identify cases of Covid-19 in the country, using technology and software originally developed for counter-terrorism purposes.

Expanding tech-focused responses to this global pandemic have also emerged in the UK. In late March, it was revealed that the NHS would be partnering with a number of Big Tech corporations, most notably Google, Amazon, and data-processing firm Palantir to develop a shared data platform to assist in Covid-19 surveillance. Understandably, this announcement has sparked widespread unease across the UK regarding the roles and motivations of these Big Tech actors, and their increased stakes in informing and assisting responses to global public health emergencies.

In recent UK memory, Google is perhaps most infamously known for the breach of data laws and privacy which occurred in the contexts of a partnership between Google DeepMind and the Royal Free London Trust, which involved the transfer of identifiable patient records across the entire Trust, without explicit consent, for the purpose of developing a clinical alert app for acute kidney injury. Of equal concern, until its partnership with the NHS, Palantir was perhaps most widely known as a data-processing firm which has continued to supply American immigration authorities with technology and analytics used for the separation of families and deportation of migrants. In seeking to alleviate public concerns centring on data privacy, as well as the role of these for-profit corporations in the UK's ongoing response to Covid-19, the NHS and UK government have continued to emphasise that tech corporations involved in the response to Covid-19 do not control the data, nor are these corporations permitted to use confidential patient data for research or commercial purposes.

Date originally posted: 2020-04-20

Permalink: https://blogs.lse.ac.uk/politicsandpolicy/tracking-covid-19/

Blog homepage: https://blogs.lse.ac.uk/politicsandpolicy/

On one hand, recent research investigating these transformations has illustrated the supplemental potential of digital disease tracking in highlighting how new data sources and technological advancements can aid in identifying and responding to outbreaks. On the other hand, these unparalleled shifts in surveillance operations also underscore the intensifying fusion of Big Tech corporations and state surveillance activities within global health security frameworks.

The political challenges and implications posed by these global transformations are, like the pandemic, unprecedented. Moreover, the rapid rise of these data-driven surveillance operations, enabled largely by tech corporations and proliferating in the forms of public-private partnerships, tracking apps, GPS devices, drones, and facial recognition technologies has unfolded amid an intensified debate of trade-offs between collective security and individual autonomy in all regions affected by the pandemic. Amid a shared sense of global emergency, innovation appears to have outpaced regulation in accounting for these expanding surveillance capacities.

Growing unease with the increasing stake held by Big Tech in assisting governments to regulate public emergencies, and concerns surrounding corporate and political interests converge in the contexts of this current global pandemic. Highly sensitive and confidential patient data held by organisations including the NHS is valued in the billions, yet the transfer of millions of records by the Royal Free to Google's DeepMind in 2015 occurred without public debate or consultation with relevant public bodies. Five years after this infamous data and privacy breach, Google has once again partnered with the NHS to assist with the development of a datastore as part of the NHS's larger project with tech corporations to track and respond to Covid-19. Yet, once more, concerned sources have drawn attention to the speed at which patient data is now being accumulated and processed by these mediums to track Covid-19, with apparent insufficient regard for privacy, ethics or data protection.

Beyond this, public scrutiny must also be directed to consider the potential 'after-life' of these technologies and new logics of big data-driven surveillance which could linger on, or be re-purposed after the pandemic has subsided. In some countries, enhanced digital surveillance capacities have been developed and launched in tandem with the arrival and escalation of cases of infections, while in other states, particularly with authoritarian governance structures, these accelerated health surveillance practices appear now as dual-use technologies, which have been hastily drafted into outbreak responses. Subsequently, these technologies cannot only trace and identify the movement of viruses, but also the movement of any surveyed population, whether during health emergencies or otherwise.

In states with stronger governance culture and institutional legitimacy, including the UK, the task at hand then for researchers, academic networks, civil society and communities will be to continually hold governments to full account on the partnerships they forge with for-profit tech corporations and security firms during states of emergency. Within these citizen-led evaluations, critical further explanations must include how and what sources of data are being collected and used, and for what purposes, and how will such surveillance operations be securely suspended, dissembled, and de-escalated following the cessation of epidemics and pandemics. In some cases, the basic question of whether such partnerships and expanded surveillance capacities should be even considered must also be asserted.

Lastly, it is critical to recall how public health emergencies are often rooted and proliferate from endemic economic, environmental, historic, social and political realities, far divorced from the tech corporations, data-warehouses and algorithms which now guide and inform the responses to emergent epidemics and pandemics. As findings from previous public health emergencies demonstrate, accelerated disease surveillance practices and the accrual of ever more personal data during outbreaks can and will fail to deliver on promises of health security and outbreak control if these new surveillance operations are not paired with continued investments with on-the-ground infrastructures, including robust healthcare systems, secure supplies of medical resources, and public trust in institutions, all of which are critical in addressing any public health risk.

It has been claimed that the Covid-19 pandemic represents a watershed moment for global health systems; a point of no return, and a needed opportunity to re-consider future directions of governance and security practices. As more and more state governments roll out increasingly opaque and digitised operations in the era of Big Data, digital disease surveillance practices and the 'creep' of tech corporations must continue to be included and actively scrutinised in assessments, evaluations and critiques of responses to pandemics, during and after Covid-19.

Date originally posted: 2020-04-20

Permalink: https://blogs.lse.ac.uk/politicsandpolicy/tracking-covid-19/

Blog homepage: https://blogs.lse.ac.uk/politicsandpolicy/

In charting a path forward for global health researchers and communities, it must be underscored that regulation of these practices, technologies and actors cannot be merely understood as an endpoint or a final destination at which we will at some point arrive at and conclude. Rather, regulation must take the form of a continued and evolving state of vigilance, scrutiny, education, cooperation, and oversight. Orientated towards the long term, the addressing of these highlighted political challenges, like the pandemic itself, will be a marathon, not a sprint.

About the Author

Stephen L Roberts is LSE Fellow in Global Health Policy in the Department of Health Policy.

Date originally posted: 2020-04-20

Permalink: https://blogs.lse.ac.uk/politicsandpolicy/tracking-covid-19/

Blog homepage: https://blogs.lse.ac.uk/politicsandpolicy/