Global Insights: COVID-19: Surveillance, Security, and Intelligence
July 20, 2020 Think Development Blog

Original post: https://blogs.warwick.ac.uk/po901/entry/covid-19_surveillance_intelligence/

Authors: Ann Fitz-Gerald, James Goldgeier, Florian Kerschbaum, Tom Sorell, Berhan Taye

Editors: Briony Jones and Maeve Moynihan

This post is part of a larger collection covering the Global Insights webinar series, hosted jointly by Balsillie School of International Affairs (Canada), the Department of Politics and International Studies at the University of Warwick (UK), the Institute for Strategic Affairs (Ethiopia), American University's School of International Service (USA), and Konstanz University (Germany). This series of Global Insights has finished and the next series will resume in September. You can access a recording of this week's webinar here.

Panellists: Ann Fitz-Gerald (BSIA), James Goldgeier (American University), Florian Kerschbaum (University of Waterloo), Tom Sorell (University of Warwick), Berhan Taye (Access Now)

COVID-19 and efforts to contain it have raised important questions about surveillance, security, and government protection of populations. The recent use of contact tracing apps in a number of countries has renewed debates surrounding privacy and surveillance and rendered them more complicated. Such apps, among other technological aspects of the pandemic like misinformation, spark important discussion surrounding the use, and misuse, of technology in the age of the pandemic.

Governments have often "declared war" on a wide range of issues, including drugs and terrorism, among others. Is COVID-19 a National Security threat? If so, how does it differ from other national security issues of the 21st century?

The crisis of COVID-19 is indeed a collective one, however we raise the question of whether war should be used for the narrative that we are facing at the moment. For those who are in the peacebuilding space, the recurring narrative of war and repetitive use of militarised language is concerning. Indeed, if the COVID-19 crisis really were a war then we would have expected those states who have invested heavily in the military, such as the USA, to have better controlled the pandemic. As such, the crisis and its narrative need not reflect the action of declaring war, but rather the action of building resilience. Whereas security is often defined as national, in that it protects a country and/or a people, recent work has expanded notions of security, including individual and societal security surrounding health, socioeconomic status, and other markers of safety. If we embrace such notions of security, the pandemic will allow us to connect demands from populations that their governments

keep them safe in many facets of quotidian life. Both the COVID-19 pandemic and the recent increased activism surrounding Black Lives Matter in the United States, the UK, and elsewhere, have demonstrated that the topic of security is not only a question of whether the government protects their people from threats, but whether the government itself becomes a threat. Thus, COVID-19 is a threat to 'national security' however not necessarily under the militarised terms in which it is traditionally defined.

We hear a lot about contract tracing apps as a tool for combatting COVID-19. How is technology being used to contain the COVID-19 virus, and what are the implications for human rights and civil liberties like the right to privacy and freedom of association?

There is an important difference to be articulated between COVID-19 surveillance, which Edward Snowden identified as part of a longer-term surveillance architecture, and other forms of surveillance related to challenges such as terrorism. The scientific basis for the COVID surveillance – in virology and epidemiology – has no counterpart in the war against terrorism. Moreover, the national health authorities, and not the government, typically collect COVID-19 data, thus separating it from traditional surveillance. However, valid concerns exist about the ways in which these tracing apps are able to change people's behaviours, and the ways in which they are becoming part of the critical infrastructure. If we consider the possibility of misuse of this app technology, we could envisage a reduction in public trust and a significant impact on public life. This leaves critical infrastructure potentially vulnerable and encourages us to think about what these apps do and what role they play. Primarily, they store and provide location and health data, and of course these databases already exist through platforms such as Goggle and Apple. One could argue that the app is a more privacy preserving solution, and a social contract for how we gather and store this information. We see, however, some challenges for democratic governments persuading their populations to use these apps. Liberal democracy has operated with a notion of a private sphere that is off limits to the government, and yet these apps require that we give up some of this privacy. In some countries, such as the USA trust in the government is already so low and it is even difficult to encourage the population to wear masks, let alone to use these apps. In others, the freedom of association and civil liberty is under threat, as the government controls internet traffic and thus can quash social movements that may be trackable through COVID-19 tracing apps. As countries around the world ease lockdown restrictions and enter a 'new normal' time will tell how this new technology will impact our societies.

Greater surveillance is a key element in the toolbox for containing the pandemic. Is there a danger that invasions of privacy will be normalized after the pandemic?

It is important to contextualise ideas and debates over privacy. There are no guarantees that this technology will not be used against the populations it purports to be serving, and we need to remain vigilant to the historical use of these technologies beyond the current COVID-19 tracing apps. This has a gendered aspect, when we consider the possibility of tracing the health choices of women in particular. Large technology companies, who provide this tracing app technology, are the same companies who have been implicated in monitoring human rights and civil liberties defenders previously. There are, of course, implications for the right to protest and the right to organise in the context of COVID-19

restrictions and surveillance during lockdown. If we look to the UK we can see increased forms and receptivity to solidarity, first with regards to the National Health Service and now with the Black Lives Matter movement. But the timing and local context matters when balancing the breaking of lockdown rules against health risks. The lived experience of many black people in the UK and the heightened sense of solidarity renders these questions particularly important. Moreover, there are questions to be answered regarding what has become normalised in these contexts of 'war'. The sharing of data between private companies and government, increased levels of police brutality, limited regulation, and government decisions without public participation are all concerning. The privacy paradox describes how we are prepared to give up privacy for a small incentive, even though we are at the same time very concerned about our private information. In the case of the COVID-19 app this paradox does not apply because it is not to the benefit of the individual but for the others who are protected if they stay at home. We should keep in mind this element when debating privacy, and acknowledge the differences between privacy concerns pre and during COVID-19.

Are there safeguards that can be enacted to ensure the technology used to address COVID do not undermine human rights?

There is significant debate as to how to construct a trustworthy app, and this is both a technical exercise as well as a democratic one. Many of the apps are being developed by those who do not have the proper expertise in privacy technology and this undermines trust in the public debate. There is a great variety between countries in terms of data protection laws and enforcement of those laws. For the human rights community this is a dangerous and worrying moment. We need oversight to generate checks and balances and public awareness of the development of such technologies. Regulators need to be at the forefront of this. We should consider whether new data laws are required, how data laws should be interpreted, and the limits of safeguards such as anonymization. This is a process of ensuring that greater technical information provides the basis of data laws. Technology of course is also not the only solution, and investment in other aspects of social infrastructure is essential. Countries will need to build communities and offer social resources to demonstrate that they are not at war and that human rights should continue to be protected.

We're also living in a world where disinformation and misinformation about COVID is rampant. Is there anything that can be done about this at national and global levels to address disinformation?

More self-conscious fact-checking resources which are prominent in social media would be helpful. In addition, the presentation of COVID updates should come from public health professionals without politicians present. We need an independent channel of communication to the wider world of public health without a partisan political spin. We see politicians and leaders who are the source of misinformation, and this needs to be countered. The issue of misinformation from a technological perspective is very difficult to handle. It is not easy to determine automatically what is misinformation, most attempts at that have failed. This is not only a technological problem but also one of a 'grand truth'

where myths may take hold and become very dominant amongst a population. Governments can help by generating transparency and involving the public in a continuous debate over privacy issues and data collection. In Germany, trustworthy actors have been used in rolling out the COVID-19 tracing app and have been involved in ongoing public discussion and this can act as an example for other countries. However, this case also illustrates the challenges of this issue as take up of the app has nonetheless been lower than hoped. There is a question of where the responsibility lies for fact-checking, whether it should be individuals or whether platforms themselves should have some responsibility. We have seen cases in Ethiopia, Kenya and Tanzania, of journalists being arrested or targeted because of sharing facts regarding COVID-19. In such sensitive contexts we need to be clear about where responsibilities lie and protections can be ensured. This requires more effective and inclusive international leadership on privacy, security and regulation during this time.

What recommendations would you make to policy makers?

1. Promote and elevate science in the discussions about COVID-19 and responses, in particular de-coupling it from politicians.
2. Use national risk registers as a point of reference as well as discuss them publicly.
3. Collect data in a transparent way, explaining to the public what you are doing and why.
4. Make policies for people at the margins.
5. The United States Government need to show more humility and commit to multilateral organisations such as the World Health Organisation.