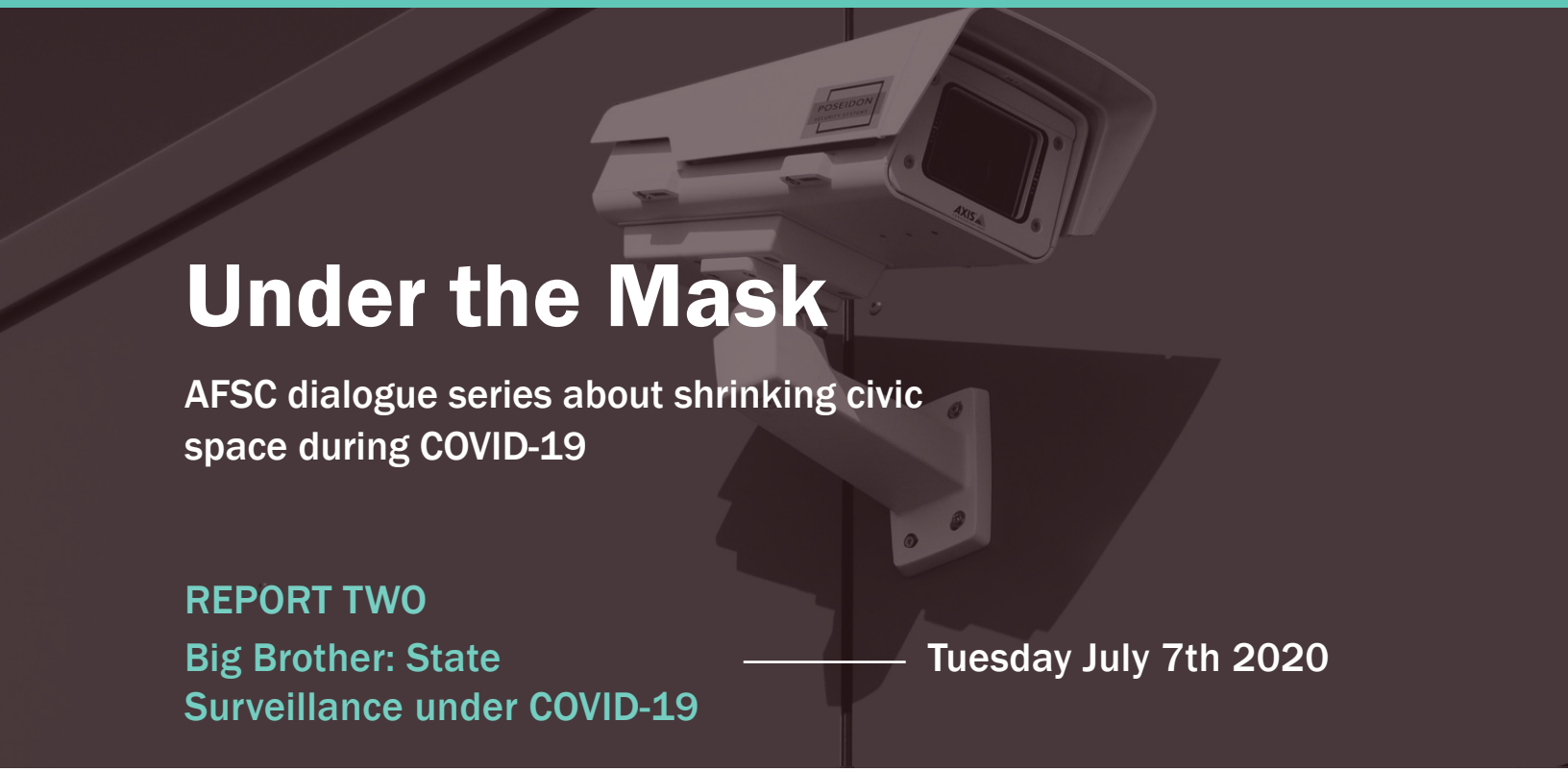

Under the Mask

AFSC dialogue series about shrinking civic space during COVID-19

REPORT TWO

Big Brother: State Surveillance under COVID-19

Tuesday July 7th 2020

The second of the four webinars in the AFSC 'Under the Mask' series considered state surveillance under COVID-19. The convening was attended by roughly 65 participants from around the globe, receiving simultaneous interpretation in Bahasa Indonesia, Spanish, and French with the presentations and the majority of the small group discussions taking place in English.

Presentations were made by:

Teresa Ma, founder and a director of Peace Generation, based in Hong Kong.
Soeung Saroeun, executive director of the Cooperation Committee for Cambodia.
Mona Shtaya, communication and campaigns specialist working in the Arab region, Jerusalem.
Samuel Ewusi, professor of Peace Studies and International Relations, based in Ethiopia.

Below is a summary of the presentations and the small group discussions that followed.

1.

Digital surveillance: What to look out for, and how is it affecting civil society?

> "The responses from African states to COVID-19 have been as diverse as Africa itself. States deploy technology in both overt and covert ways to provide state and human security—sometimes for good, other times for ill. Sophisticated technological applications with the capacity to collect personal and group information pose serious threats to individual freedoms and can be used for oppression and suppression—enabling traditionally oppressive to intrude on individual freedoms. Ethiopia only has one mobile service provider, so it is quite easy to collate personal data from a range of citizens. Other countries collect data from targeted people. While Ethiopia, Rwanda and South Africa have more advanced methods of surveillance, most countries do not have such capacity.
>
> —*From the presentation of* **Samuel Ewusi**

Under COVID-19, we are seeing **a huge increase in state location tracking** (for contact tracing) across the globe.

AFSC undertook an informal survey. **Of 34 respondents** asked if their government was using mass surveillance during COVID-19, responses were evenly spread between yes, no, and don't know.

SURVEY QUESTION:

Select all the surveillance measures that the government in your country has implemented?

Phone location tracking: 9
Facial recognition: 3
Electronic bracelets: 0
Personal bar-code systems: 2
Drones: 4
Other: 4

Many states have revealed that they already had these capabilities. Others are currently acquiring them with strong narratives about how these technologies were successful in containing the virus in other places. Companies that trade in digital big data are looking to exploit new markets, which is a concern of its own. **While there are legitimate public health uses of such tracking, the danger of overreach is always present, especially where there is a history of authoritarianism. The discourse about surveillance under COVID-19 is once again dominated by the false dichotomy of security vs. freedom.**

In addition, we are seeing **non-state big-data information-gathering growing** (such as the example of food delivery companies presenting themselves in the business world as big-data companies and selling people's culinary preferences)—and we are seeing states gathering much more than just location information. **Personal information gathered by states can include pictures, texts, emails and much more, and on many occasions has been used to threaten activists and their relatives long before COVID-19. Under COVID-19,** governments are also collecting more health and employment information, using "voluntary apps" that demand citizens' permission to share the data in exchange for certain services, or for state employees. This has already been used to repress certain populations or **contribute to racist narratives against them, and surveillance technologies are also being acquired to trace migratory movements.**

> "
>
> Big Brother surveillance has long been a part of daily life in Palestine. The Israeli government, and to a lesser extent the Palestinian Authority, keeps Palestinians under surveillance as well as visitors. The government profits from selling surveillance equipment internationally, and the Israeli Secret Service has been spying on Israeli citizen communications since 2002. In March, they launched a mobile phone tracking technology to trace Israelis diagnosed with COVID-19, and the Supreme Court has allowed this to continue as long as a parliamentary group oversees the program. Palestinians entering Israel must download an app that allows the military to track their calls, notifications and phone files, and many other Palestinians have downloaded the app without realizing the access it gives the government. Companies and governments are fighting for citizens data. In response civil society needs to raise awareness of the right to privacy.
>
> ***—From the presentation of* Mona Shtaya**

It is important to note that when we talk about state surveillance, it's not only a question of spyware, hacking into phones, or other forms of access to private information, but also **what kind of information we choose to make public, especially over social media, and how it is collected—and used against us.** Under COVID-19 we have seen a global increase in the number of people being investigated, and even imprisoned under a new wave of "fake-news" laws that in effect criminalize different forms of criticism against the government—including things as small as Facebook posts and digital footprint. Now, when so much of our activism has moved to the digital world due to social distancing, this problem increases.

States using surveillance against activists and minorities (and now under COVID-19 using quarantine and other new methods against activists, journalists, and whoever else is determined to be a threat) not only puts people's private information and organizing in the hands of governments, but also **has a chilling effect of intimidating civil society and causes activist groups to waste valuable energy in keeping safe instead of struggling for social change.** It is also important to note that often these systems are paid for by third party countries (such as the U.S., China, or EU) and we need to ask what are the interests and neo-colonial structures that come with them.

> "
>
> The UN High Commissioner for Human Rights reports that in the name of COVID 19, the Cambodian authorities have arrested at least 30 people, including journalists, for spreading "fake news" about the pandemic. Ten of these are associated with the main opposition party that the current government, in power since 1998, dissolved in 2017. The movement of foreign visitors and residents are also being tracked through the "Foreigners Present in Cambodia System" app. Media licenses for news agencies have been revoked, and a number of Facebook accounts have been closed. Civil society organizations, especially media organizations, reporters, editors, and rights groups, have expressed serious concern over the restricting environment and curtailment of freedom of expression.
>
> ***—From the presentation of* Soeung Saroeun**

Beyond the misuse of information by states, there's also a real concern of **data breaches, how this information is stored, and who has access to it.** Around the world there have been countless cases of security service employees using private information for their own personal use and selling of private information. Regime changes can result in information changing hands from what used to be a democratic government to what in the future may be an authoritarian one. While there is a strong narrative that if you do nothing wrong you have nothing to be afraid of when it comes to surveillance, what is considered "wrong" may change very quickly, and what can be done with information about us can go far beyond the question of whether one is a law obeying citizen.

Lastly, it seems that governments are now increasing investment in surveillance technology as opposed to other public health needs, and passing legislation to solidify these initiatives in a time where public criticism is more difficult and the voices of communities with less access to the internet are absent from the conversation.

2.

How do we shift the discourse around surveillance, and limit it?

First there is a need for more **awareness in civil society and wider circles about the quantity of information we give corporations and governments on a daily basis** through our use of digital devices. This can come with a list of good practices, practical tools, and open source software that can help keep us safer.

> “
>
> Hong Kong is technologically advanced with sophisticated telecoms systems and 94% of households having broadband. CCTV is a standard feature not just in public spaces but also business and residential buildings and even some private homes. When the government added COVID-19 to the notifiable list of infectious diseases, personal data protection at law loosened. It meant there was no longer a need to gain consent for the use of personal data for a new purpose and people’s right to access personal data stored by a state agency was suspended. The government is using electronic wrist bands and smart phone apps to track quarantined people. The level of intrusion does not feel excessive. However, surveillance by the private sector went up during the pandemic and people are much less vigilant about non-state surveillance and the type of data collected by the private sector, which can be more intimate and can include political views, DNA test results, travel, financial information and so on.
>
> ***—From the presentation of* Teresa Ma**

On the question of mass collection of personal data, its sale, and its use by governments to suppress opposition, there is a need for **ethical guidelines that can be advocated for to both legislators and social media operators.** This could be done through creating a civilian oversight board. Specifically, around COVID we should compile guidelines for legislation balancing public health and civil rights to be used as an advocacy tool by civil society. This should include governments being transparent about the data they store, the use they make of the information and who has access to it, as well as having it run by the ministry of health.

Data protection needs to be treated like other human rights, and we need to call for an international law framework, through treaties, conventions, and other means.

On a larger level, it is important that we challenge the current narrative that presents communities and people as needing to be controlled in order to combat the virus. Instead we can **emphasize the strength and resilience arising in collective community action and identify how to work with, and not on, communities to control the spread of the virus, and not to control people.** This should also be reflected in allocation of budgets to the health sector rather than militarism, including surveillance.

3.

Civil society strategies and tools to mitigate state surveillance:

- Digital safety guidance, training and updates from the tech community about weaknesses and strengths of various apps and communication tools.
- Build community-owned and managed information collection about COVID, to keep the tracking in the community.
- Collect and develop information on who (governments, companies, etc.) is behind the management of our data, and what they do with it (with an emphasis on private corporations and their financial benefit from information harvest) to allow for economic activism campaigns.

Resources:

The Digital Transnational Repression Toolkit, and Its Silencing Effects | Freedom House

Safer software recommendations:

- Signal: a direct messaging app (like WhatsApp but safer).
- Email: Proton Mail, Tutanota Mail.

Appendix 1:

Tracking location and infection

Tracking the places that COVID-19 infected people have been, before being quarantined and/or hospitalized, is extremely important to fight this epidemic. But here's why phone geolocation mass data collection tools are not the right way to do it:

1. Privacy. Our private information should be private, and when it isn't, it can be sold for profit or used against us by the state, or even just by individuals who gain access to it.
2. Normalization of intrusive measures after COVID. We're already seeing countries legislating and legitimizing surveillance for the long run, not just as an emergency response now.
3. If governments and secret services identify possible infections and send people to quarantine based on confidential information, how do we know they won't use it for their own political gain?
4. Automated systems are crucial when dealing with big data. And automated systems make mistakes. These mistakes can send thousands to forced quarantine with no due process.
5. Mass geolocation tools don't know walls, doors, or even depth, and again, send people to quarantine based on this.
6. Different governmental and private bodies will have access to this information, which can both lead to leaks and be misused by people with access. When we talk about corporate bodies, it is likely that this information will be used to create profit for them in the future as well.

All of these together create distrust in government, in a time when we really need to be able to trust our government.

Alterative solutions are already in place:

1. Voluntary apps are voluntary, and so rely on a trusting relationship but also equalize the power-relation between state and citizen – we need each other. But these need to be actually voluntary (without conditions).
2. Any collection of data should be collected on the individual's phone (not uploaded to a cloud) so that information stays private and leaking of information is prevented.
3. Open source apps allow the public to trust them and the way they are used, and collectively make them stronger and safer.
4. There should be full transparency about who collects what information and what bodies then have access to it. A civilian monitoring board may be a way to assure that.
5. A clear timeline must be set indicating from when and until when information is saved, how it will be deleted, and when all forms of data collection on COVID to an end. It must be health professionals making these decisions.