Digitalization in the Corona Trap

Why voluntary mobile phone tracking does not work

In the fight against the coronary crisis, voluntary apps are now supposed to help, which warn their users supposedly anonymously when they come into contact with infected persons. In this way, it should be possible to relax lock-down restrictions. This approach will fail, comments Stefan Brink, the state data protection commissioner of the state of Baden-Wuerttemberg in Germany, and Clarissa Henning in their following article. (Originally published in German on 3 April 2020, https://netzpolitik.org/2020/warum-freiwilliges-handy-tracking-nicht-funktioniert/ , informal translation by ICS Centre)

Germany shortly before the first massive pandemic wave: We understand that this virus cannot be stopped permanently in its exponential spread, that we cannot identify and interrupt chains of infection as before, that our health system will not be able to save thousands of people, mainly from risk groups. As helplessness increases, so does the demand "that something must be done".

Something is quickly found: digital technologies should put us back in charge, make us "master of the situation", and thus contain the fear of the unmanageable danger. In doing so, we overlook the fact that we still cannot win the battle against the virus this way - and that we are also putting our freedoms and the rule of law at risk.

The search for a quick saviour

In the absence of an effective vaccine, alternatives must of course be considered and tested: Social distancing, sanitation measures, lock-downs. However, an effective separation of risk groups from the virus does not seem practically and politically feasible, so the focus is turning to the infected (and soon also to those suspected of infection). They are to be identified via tests and then quarantined by the health authorities, which will then be surveilled and tracked as closely as possible if necessary.

First, the Minister of Health, suggested new laws which were nothing less than a massive intervention into the human rights of infected persons by using their location and telephone traffic data. This attempt was fenced off but the call for a "digital" solution to the health crisis is getting louder again. "Voluntariness" is now to replace coercive measures, and there is talk of "anonymised information flows".

Both approaches appear modern and fundamental rights-friendly, but on closer inspection they are neither: in times of crisis, people look for a quick saviour – and it's not our health system since it shows its obvious limitations. And as pharmaceutical research still needs more time, which the risk groups do not have, then it should be something great, gorgeous and misconceived, such as digitalization, that saves us.

Digitalization refers to the conversion of analog values into machine-readable "digital" formats and their processing by information technology. With it, more and more previously invisible, highly complex processes of real life are being recorded and made readable by means of technical sensors and are thus relevant for the control and design of human behaviour.

This applies to the intelligent refrigerator as well as to the self-driving car. For the current situation, this means that if the everyday life of everyone is documented using digital technologies, knowledge could be extracted, in order to control the invisible and highly complex process of

spreading of the virus and brought under control by "digital measures".

Period. The end of digitalization

However, this is a misconception that tells more about our unwavering faith in technology and our acute desperation than we should wish for: There is no technical sensor technology that allows us to trace or concretely predict the path of individual virus infections. Full stop. No more digitalization.

What exists are attempts to technically record human behaviour - especially that of infected and suspected persons - and to make the data usable in the fight against the pandemic. Word has got around that the use of GSM location data is far too imprecise for this purpose and even the GPS location data recorded by smartphones is not good enough. However, this data does not determine the radius of infection, nor does it depict the fact that we are not only moving next to each other but also on top of each other in multi-story buildings, underground trains and shopping centres. Whereas the data might indicate close contact, we could be "safely" separated by walls or windows even when it shows that we are in the same location.

That is why Bluetooth technology is being suggested, whose weakness could now be turned into a strength: It only extends a few metres and, thus, correlates best with the infection radius of 1.5 to 2 metres proclaimed by virologists. Hence, from mid-April, a "tracking app" will be available that automatically exchanges anonymized data via Bluetooth LE numerical codes with the smartphones of those people around us to whom we have come so close that infection could have been possible. A positive Covid-19 testing result would trigger that all stored codes in the memory of the smartphone of the infected person would be automatically transmitted to a central server.

Unfortunately, upon reflection this hope for salvation dwindles: Bluetooth technology, depending on the environment, is simply unreliable: Sometimes it barely reaches one meter, sometimes and under the most favourable conditions, up to one hundred meters. In the latter case, its footprint is far too large to derive realistic information about infection risks. Not to mention the practical problems of having a smartphone in your back pocket emitting different radiation than one in your hand. Add this complication, in a large apartment building you may live wall to wall with an infected person whom you have neither met nor will ever meet. At this stage, predictions of being able to intercept such imponderables of Bluetooth use through signal strength measurements are yet to be confirmed.

Doubts about anonymity

The technical solutions presented for the anonymity of the exchanged data also raise obvious doubts: the numerical codes can only be *pseudonymised,* i.e. information that can still be related to a person, and not *anonymised* if the aim is to identify persons at risk of infection.

This also means that at least for the owner of the mobile phone it is potentially readable which concrete persons are behind the codes that are stored in her/his memory. She/he could easily assign to the numeric app code to a certain person known to her/him, whom she/he met during the incubation period. The promise made by the app developers to give top priority to anonymization for data protection purposes should therefore be reviewed again.

But apart from these details, we also need to look at something else: the aspect of voluntariness in the use of tracking apps. It is doubtful whether everyone is willing to install the app. The mistrust of state and private surveillance has been massively fueled in recent years, Facebook scandals and illegal online tracking have left their mark as well as misconduct by the authorities, most recently when the Police (in some German states) obtained illegally the personal details of infected persons

for "self-defense".

Voluntariness looks different

Let us, for the sake of the argument, assume that the current uncertainty among the population actually leads to "almost 100 percent" downloads of the app, as the Finance Minister expects. Such "expectations" already trigger pressure on the population that counteracts any sense of voluntariness. Especially since the subtext is also clearly noticible: relaxation of the contact restrictions and lock-down is linked to the willingness of citizens to participate in self-tracking. If the voluntary approach does not work, the government may again resort to coercive measures. Especially in the current situation, voluntariness looks different.

Hence, it seems that a debate on voluntariness is going on where the outcome is already a foregone conclusion. And, let us remind ourselves that "100 percent of the population" do not posses an app-enabled mobile phone, and among the risk groups in particular, there is a lack of apps in well over a third of the devices.

How should such expectations of readiness and effectivenes ever be fulfilled? Or are we already thinking about measures to "promote" the "voluntariness" of participation in app tracking: We are aware of the reports from Wuhan, Singapore and Hong Kong, where using public transport or shopping at the supermarket, is contingent on whether the app is activated or not. Here, at the latest, voluntariness clearly ends.

Voluntary tracking apps will fail

However, a completely different (human) factor will be decisive: The human psyche will make voluntary tracking apps fail. Individuals will install the app expecting to gain an advantage from its use, namely information about relevant contacts with infected persons. Now, if that person receives the message about her/his own infection the reasoning is likely to change: she/he no longer sees an advantage from informing others about her/his infection status, and must even consider additional risks that could emanate from the app operator, government agencies or even contact persons, who might try to identify her/him despite the guaranteed anonymity of the app.

So how many of the app users will share this information, which is so important for others, in solidarity? Can the app now be uninstalled again or has the right of revocation (and thus voluntariness) expired with the infection? Or do you “out” yourself by uninstalling the app, since the assumption that there is "nothing to hide" no longer applies?

Let's take a look at the second type of user - the non-infected app user - who receives a message about a contact with somebody who has fallen sick and, thus, is followed by a request to place herself/himself in domestic quarantine. The app user is free to comply with the quarantine order as she/he wishes, and this is where the app's promise of anonymity comes into play for the second time.

"Quarantine yourself"

With a rate of less than 0.1 percent of positively tested citizens, messages such as "Go into quarantine" are rarely expected at first - but what if we have 30 and more percent of (formerly) infected persons on the way to what is called herd immunity? Who then voluntarily goes into domestic quarantine for the third or fourth time, just when she/he does not feel sick, knows about the weaknesses of Bluetooth technology and it is up to the person alone whether to abide to the message or to delete it?

Better than nothing, one might think, a certain number of citizens will install and use the app, and will honestly pass on their own infection and use such messages as a reason to withdraw from public life without complaint. But nobody should forget that this "social experiment" is not a leisure time event, but takes place during a very serious health crisis, followed by a serious economic downturn: Every failure costs time, energy and trust and might even endanger human lives.

It is sobering for a data protection militant to face the truth: Voluntary tracking apps do not have the technical, legal or social potential to succeed. Let's therefore turn as early as possible to the necessary debate that lies ahead of us: Under what conditions may positively tested persons be monitored so as to ensure compliance with the quarantine obligation? Will we succeed in limiting the surveillance measures in accordance with the constitution to those who are in recognizable violation of regulations, or will compulsory measures - keywords: electronic wristband and geofencing - be imposed on all potential virus transmitters who represent a potential risk for their fellow human beings because of their infection?

The resilience of our liberal democracy will be demonstrated by this question - not by the usage rate of an allegedly voluntary tracking app.

Translation by Karl Steinacker (with assistance of DeepL)