DIGITAL CONTACT TRACING IN NORWAY

The health authorities' strategy for opening Norway after lockdown is targeted testing, isolation, contact tracing, and quarantine.

Contact tracing is essential but challenging. For instance, we tend to quickly forget where we have been, and whom we have been near. Moreover, many individuals who infect others have few or no symptoms.

To date, contact tracing has been performed as laborious manual work, mainly through telephone interviews. However, this practice scales poorly and is both time and resource consuming.

Digital contact tracing

Smartphones can register locations as well as other phones nearby. The idea behind the contact tracing apps is to use this information to track and notify about infections. For instance, when a user is confirmed infected by Covid-19, the system can identify where this person has been, and whom the user has had close contact with.

The tracing apps can immediately and automatically notify all close contacts that the system detects. A reduction in response time to trace probable Covid-19 patients from days to minutes might prevent new infections considerably.

On April 15th, the Norwegian Institute of Public Health (NIPH) launched the app *Smittestopp*, developed by Simula Research Laboratory. On June 3rd, there were 592,924 active users of *Smittestopp*. The app was initially tested in selected municipalities to evaluate if it could identify more close contacts than manual contact tracing.

Smittestopp is now temorarily banned due to privacy concerns. See end note.

SUMMARY

- Digital contact tracing can provide earlier notifications to potentially infected individuals, as well as an overview of how the virus is spreading, and whether the measures against it are working. However, the usefulness of tracing apps remains uncertain.
- In April 2020, the Norwegian health authorities launched the app Smittestopp to collect and store sensitive data about users' state of infection, location, movement, and close contacts. The app was voluntary and time limited, and location data would be automatically deleted after 30 days.
- The Norwegian app opted for centralised data storage, to enable faster and more precise contact tracing. Most European countries have chosen a decentralised model due to privacy concerns.
- Smittestopp had three purposes, but these were neither specified in the regulations nor in the users' declaration of consent.
- Anonymous data from digital tracking can be re-identified and should not be used by others than the health authorities.
- Whether open source is the best strategy to make the app secure is debated by experts.

Privacy concerns and the Smittestopp app

Smittestopp collected and stored users' state of infection, location, movement, and close contacts. These data are personal, sensitive, and challenging to anonymise. Such data should, in line with the GDPR privacy regulation, be collected to a small extent and be well protected.

The processing of personal data in *Smittestopp* was regulated by a new regulation for digital contact tracing and epidemic control, which lasts from March 27th, to December 1st, 2020.

All citizens who are infected by the Coronavirus are required to assist with contact tracing. However, digital contact tracing was voluntary. The user was able to temporarily disable tracking and uninstall the app at any time. Moreover, personal data could not be used to control whether individuals complied with advice or orders, nor could they be exploited commercially.

According to the Norwegian Institute of Public Health (NIPH) location data would be be automatically deleted after 30 days. When the user deleted the application, all personal data about the individual must be deleted or anonymised.

The pandemic is expected to last longer than December 1st, 2020. This raised questions about the criteria for an extension, and what defines the end of the pandemic.

How accurate is automatic notification?

In order to optimize the value, the infection must be contained as much as possible, but with few unnecessary costs such as quarantine for healthy individuals.

Automatic infection notification is based on one standard definition of "close contact" to trigger an alert. *Smittestopp* adopted the definition given by the Norwegian Institute of Public Health (NIPH): Close contact means less than 2 meters distance lasting for more than 15 continuous minutes with a person who is confirmed infected by Covid-19.

However, smartphones do not necessarily measure the distance between people. In reality, the infection risk will vary based on the situation. This can reduce the usefulness of automatic contact tracing in two ways:

Low specificity means that users get a notification even if they are not infected (false positives). For instance, a heap of school bags containing phones will be measured as close contacts, even if the individuals keep a physical distance. Neither do smartphones register whether there are protective screens, walls, or floors between the close contacts. False alerts might increase the demand for tests, cause unnecessary quarantine, and fear among the population.

Low sensitivity means that users do not get notified even if they are infected (false negatives). Smartphones are not able to understand the characteristics of the environment that may affect the risk of infection. For instance, poor air ventilation at choir rehearsal may pose a risk of infection, even if distance and duration are not defined as close contact. This can lead to false sense of safety and an increased risk of infected persons spreading the virus to others.

In a broad sense, sensitivity also depends on the percentage of the population using the app. The more confirmed infected individuals who used *Smittestopp*, the more close contacts could be notified quickly. In order for many people to download the app, they must find it useful. Precision and distribution are, therefore, mutually dependent factors.

Uncertain benefits from digital tracing apps

Although several countries are using digital contact tracing, or are planning to do so, it has not yet been documented that this results in lower infection rates. Norway was an early adopter, which made it necessary to make continuous assessments of whether the benefit was in proportion to the costs for the citizen and society.

Hence, the rules that define close contact must be re-adjusted, as we gain more knowledge about how Corona infections occur, and how the smartphone as a tracing tool operates in practice.

How many of the close contacts that are false positives is an integral part of the assessment. Moreover, estimates should also be made of the number of infected individuals not detected by the app.

The recommendations in the automatic notifications should be proportionate to how specific the app is. It is reasonable to assume that there will be a considerable number of false positives due to the sources of error. Instead of recommending quarantine, close contacts can, for example, test themselves. From this point of view, the most crucial function of digital contact tracing is to prioritise who should be tested.

Smittestopp could also function as a support tool for manual contact tracing. It could register where infected users have been and whom they have met. A human contact tracer can source false positives and identify cases that might otherwise have gone under the radar. However, this would require allowing such actors to access sensitive data from the app.

A separate consent for each purpose?

Smittestopp had three distinct purposes. According to the regulation, it should contribute to *rapid tracing and dissemination of advice* to individuals who may be infected by the coronavirus SARS CoV-2. Furthermore, *surveillance at the population level* should help monitor the prevalence of the virus and evaluate the effect of infection control measures.

Simula's website expressed the third purpose: gather *anonymous data for research* to be better prepared for future pandemics.

These three purposes can bring societal benefits. However, each purpose demands different types and amounts of data. It has been challenging to assess whether the handling of information was necessary to achieve a particular purpose, as NIPH did not clearly distinguish them. The health authorities should describe what effects they aim to achieve for each purpose and how they will utilise various types of data for this.

The user could only give one consent for all three purposes, which would allow for more extensive use of data than solely contact tracing. It would strengthen privacy if the user could choose to give consent to the various purposes separately.

Resale of anonymous data

According to Bent Høie, the Minister of Health and Care Services, reusing anonymous data is essential for value creation and innovation. Moreover, Høie states that there "are no specific restrictions in the regulations for the sale of anonymous, aggregated data."

In line with the development of intelligent data analysis and machine learning, it becomes possible to derive more information by connecting several anonymised datasets, which can cause individuals to become re-identifiable.

In case anonymised data gets connected to large datasets at major international companies, Norwegian citizens may be re-identified. Thus, resale of anonymous data from contact tracing apps should consequently be reconsidered.

Is location data necessary?

There are two ways to register close contact that are relevant for digital contact tracing:

- Bluetooth is a feature of mobile phones that can detect other phones within a range of about 10 meters. The signal strength indicates the distance.
- GPS *(Global Positioning System)* is a satellite-based system that can locate a phone with an accuracy down to 2-7 meters.

The user must actively allow the use of Bluetooth and GPS tracking. *Smittestopp* used both GPS and Bluetooth to calculate proximity to other phones. Simula stated that this combination gives the best accuracy. However, the European Data Protection Board (EDPB) highlight that contact tracing does not require GPS tracking of individuals, and that such gathering of data violates the principle of data minimization. Data minimization involves limiting the amount of personal data to what is necessary to realise the purpose of data collection.

Centralised or decentralised storage?

Contact data can be stored in two different ways. With *centralised solutions*, information about close contact is collected by the health authorities. When someone is confirmed infected, the authorities immediately notify those who have been in close contact with the Covid-19 patient. Authorities are also allowed to monitor developments and update their strategies continuously.

Smittestopp was a centralised solution. At the time of lauch, Simula pointed out that the utilisation of data was well adjusted in the regulation for digital contact tracing. Moreover, Simula stated that central storage provides faster and more precise contact tracing, and a better understanding of the effect of various measures. Additionally, it contributes to research for grasping future epidemics. Centralised storage can also be convenient if digital contact tracing is combined with manual tracing.

Decentralised solutions have been chosen in other European countries such as Germany and Denmark.

This solution implies that contact information can be stored anonymously and encrypted in each user's phone. When someone is confirmed infected, the system calculates whom it will notify under the programmed rules. No third parties need access to the data.

Google and Apple have collaborated in developing such solutions that notify close contacts while storing data locally on mobile phones. The system should also allow users to exchange and measure proximity more precisely and across different phones with Bluetooth. Google and Apple offer an interface for this, while each country develops and operates its own contact tracing apps. A common approach will also be advantageous for cross-border use.

Nevertheless, this solution cannot be used with GPS data, and prevents authorities from accessing the data. French authorities are sceptical of handing over technology decisions to large commercial actors with considerable self-interest.

The European data protection board states that both centralised and decentralised data storage can be valid alternatives. However, decentralised solutions are perceived as the best solution for data minimization.

The expert group that evaluated *Smittestopp* suggested considering a more decentralised solution when the trial period was over. This may be less privacy intrusive, which could increase the use of the app.

Closed or open source?

Within IT development, it is not uncommon for source code to be openly published. In this way, more eyes will be able to assess different issues, improve the code, and possibly reveal security weaknesses.

On the other hand, having security weaknesses revealed may lead to misuse or exploitation by malevolent actors. NIPH chose to keep the source code for *Smittestopp* closed, referring to security risk and the danger of misuse in case the code fell into the wrong hands.

There is disagreement in the professional and academic community about whether this is the right strategy. The European data protection board suggest that the source code should be open to facilitate a broad examination by the research community.

The Ministry of Health gave the expert group access to the source code to evaluate privacy, security, and potential vulnerabilities. Their report suggests that as much as possible of the source code should be available as open source, so that users get a real and direct insight into how their data is managed.

Updates

On June 12th, the Norwegian Data Protection Authority notified the Norwegian Institute for Public Health that they would temporarily ban the processing of personal data related to Smittestopp. The DPA believed that Smittestopp cannot be considered a proportionate intervention in the user's privacy. In addition, they stated that GPS tracking does not follow the privacy regulation's principle of data minimization. Moreover, DPA was also critical of the fact that a single user's consent applies to different purposes.

On June 16th, the Parliament voted that Smittestopp needed to be changed, in order to enable users to provide separate consents for contact tracing on one hand, and knowledge acquisition on the other.

On September 28th, the Norwegian Institute for Public Health announced that they will terminate Smittestopp. Instead they will develop a new app, based on the Exposure Notifications System framework developed by Apple and Google

Authors: Tore Tennøe / Hilde Lovett
Published: June 2020, updated September 2020
Contact: post@teknologiradet.no / www.teknologiradet.no

The Norwegian Board of Technology advices the Norwegian Parliament and Government on new technology.