AMNESTY INTERNATONAL

www.amnesty.org

e: contactus@amnesty.org
t: +44-20-74135500
f: +44-20-79561157

1 Easton Street,
London, WC1X 0DW,
United Kingdom

AMNESTY INTERNATIONAL

To Monica Maeland
Minister of Justice and Public Security
The Ministry of Justice and Public Security
PO box 8005 Dep
0030 Oslo
Norway
E-mail: postmottak@jd.dep.no

Copies to:
Norwegian Institute of Public Health
E-mail: folkehelseinstituttet@fhi.no

Norwegian Data Protection Authority
E-mail: bet@datatilsynet.no

By E-mail

2 June 2020

Dear Minister,

CONCERNS REGARDING THE GOVERNMENT OF NORWAY'S SMITTESTOPP APP

I am writing to you with regards to an ongoing research project Amnesty International is conducting on COVID-19 contact tracing apps around the world. Amnesty International has surveyed apps from around 15 countries so far, including Norway's Smittestopp app. This has involved a technical analysis of each app in order to understand its features and to check that appropriate privacy protections are in place to protect the human rights of users.

While we recognise all the efforts and actions taken to contain the spread of COVID-19 pandemic, we would like to urgently bring to your attention serious concerns we found regarding the Smittestopp app introduced by the Norwegian Institute of Public Health. The app has, so far, been downloaded by more than 100,000 users.

Over the last week, Amnesty International has analysed the Smittestopp app and found that it is one of the most privacy invasive apps amongst those that we analysed. Amnesty International already has serious concerns about the roll out of contact tracing apps that are not carefully designed to be compliant with human rights. We have publicly spoken out about contact tracing apps around the world, including in Australia, China, France, Italy, the Netherlands, Qatar and the UK.

In order to be human rights compliant, contact tracing apps must, among other things, build in privacy and data protection by design, meaning any data collected must be the minimum amount necessary, and securely stored. All data collection must be restricted to controlling the spread of COVID-19 and should not be used for any other purpose - including law-enforcement, national security or immigration control. It must also not be made available to any third party or for commercial use. Any individual decision to download and use contact tracing apps must also be entirely voluntary. There must also be transparent scientific proof that it is impossible for collected data to be de-anonymised, including by combining it with other data sets. Please refer to Appendix B below for details.

In this case, Amnesty International's Security lab identified the following features of the app that are highly concerning from a privacy perspective and do not comply with several human rights standards outlined above:

- The app requires registration with a valid phone number. Thus, the operators of the app can tie any data upload to an identifiable individual.

- The app collects GPS data. It stores a local copy, but also uploads this data to a central server. This allows operators of the app to track movement and location data of thousands of people who have the app installed. The Smittestopp app thus has the potential to be a mass surveillance tool.

- The app also uploads all user data to third-party Microsoft servers, which appear to be operating in Ireland.

- The app also performs Bluetooth-based contact tracing. Apps running on devices in the proximity will exchange the respective unique identifiers and store them locally, along with a timestamp and signal strength. These records are also uploaded to the central server. This data is thus neither anonymised, nor decentralised, allowing app operators to track users' movements making it a privacy violation. Additionally, the use of unique identifiers could enable malicious actors to track users' movements using a distributed network of Bluetooth sensors. This is a privacy risk.

Given the grave privacy risks to thousands of people, we wanted to alert you to this and urge you to immediately roll back the app in its current form and ensure that any contact tracing efforts are human rights respecting.

Due to the scale of privacy concerns to all users of the app, we plan to make our findings public as soon as possible. We therefore await your response by close of business on 9 June 2020.

Yours sincerely,

T O'Carroll

John Peder-Egenæs.

Tanya O'Carroll
Director, Amnesty Tech

John Peder Egenæs
Director, Amnesty International in Norway

APPENDIX A: TECHNICAL FINDINGS

- The application uses Microsoft Azure IoT Hub, which is a Microsoft platform to manage communication between Internet of things devices and the Microsoft Azure cloud. As such all the data from the app is sent to a Microsoft server, that is seemingly located in Ireland.

- The app requires a phone number to register. It registers with the IoT Hub backend, which returns an access key and a unique device identifier:

```
{
   "ConnectionString": "HostName=iot-smittestopp-prod.azure-devices.net;DeviceId=[REDACTED];SharedAccessKey=[REDACTED]",
   "DeviceId": "[REDACTED]",
   "HostName": "iot-smittestopp-prod.azure-devices.net",
   "PhoneNumber": "+44",
   "SharedAccessKey": "[REDACTED]"
}
```

- The app uses Android's Location interface in order to listen to GPS location updates, store a local copy, and eventually upload records to IoT Hub.

```
timber.a.a.d.c('(' + var_location.getLatitude() + ", " + var_location.getLongitude() + "), accuracy: " + var_location.getAccuracy(), new Object[0]);

long v7 = var_location.getTime() / 1000L;

double v2 = var_location.getLatitude();

double v4 = var_location.getLongitude();

double v9 = (double)var_location.getAccuracy();

double v11 = var_location.getAltitude();

double v13 = (double)var_location.getSpeed();
```

- The app initiates a Bluetooth Low Energy (BLE) advertiser providing access to the app's unique identifier. When a near-by device wants to register a contact with a user's device it will request the unique device identifier. The list of near-by devices identified is sent regularly to Microsoft IoT Hub. Because the identifier for a device is unique, it is possible to retrace on the server side the contacts between people using the application. Although it would require a network of Bluetooth sensors, it is technically possible to use this unique identifier to track user’s movement in an area.

Appendix B: Human Rights Principles for Contact Tracing Apps

Amnesty International has highlighted seven key principles that should guide the government's decisions before a full roll-out of any contact tracing app:

1. Consent and transparency
Any individual decision to download and use it must be entirely voluntary and the full source code underlying the app should be available for scrutiny.

2. Limited purpose
All data collection must be restricted to controlling the spread of COVID-19 and it should not be used for any other purpose - including law-enforcement, national security or immigration control. It must also not be made available to any third party or for commercial use.

3. Anonymity
There must be transparent scientific proof that it is impossible for collected data to be de-anonymised, including through combination with other data sets.

4. Privacy and data protection by design
The app must be in line with relevant data protection laws, with privacy at the forefront. Data collected must be the minimum possible, and securely stored.

5. Independent expert oversight
The app and collection and use of data must be independently overseen by a regulator empowered to enforce its decisions.

6. Time limits
The data and app must be subject to mandatory time-bound deletion and/or deleted as soon as practicable after serving their declared purpose.

7. Equality and non-discrimination
The collection and use of data through the app must not impact disproportionately on any individual as a result of their particular status, such as socioeconomic or immigration position, age or ethnic origins. Moreover, its benefits should be equally accessible to all, accounting for differentiated access to smartphones and similar.