AMNESTY INTERNATIONAL

PRESS RELEASE

EMBARGO: 00:01 BST WEDNESDAY 17 JUNE

Bahrain, Kuwait and Norway contact tracing apps among most dangerous for privacy

- Analysis of coronavirus apps in Europe, Middle East and North Africa finds major risks for human rights

Bahrain, Kuwait and Norway have rolled out some of the most invasive COVID-19 contact tracing apps around the world, putting the privacy and security of hundreds of thousands of people at risk, an Amnesty International investigation reveals.

Amnesty's Security Lab reviewed contact tracing apps from Europe, Middle East and North Africa, including a detailed technical analysis of 11 apps in Algeria, Bahrain, France, Iceland, Israel, Kuwait, Lebanon, Norway, Qatar, Tunisia and United Arab Emirates, some of which ranged from bad to dangerous for human rights. Bahrain's 'BeAware Bahrain', Kuwait's 'Shlonik' and Norway's 'Smittestopp' apps stood out as among the most alarming mass surveillance tools assessed by Amnesty, with all three actively carrying out live or near-live tracking of users' locations by frequently uploading GPS coordinates to a central server.

"Bahrain, Kuwait and Norway are running roughshod over people's privacy, with highly invasive surveillance tools which go far beyond what is justified in efforts to tackle COVID-19. These governments must immediately halt the use of such intrusive apps in their current form," said Claudio Guarnieri, Head of Amnesty International's Security Lab.

"These three apps are just the tip of the iceberg. They are essentially broadcasting the locations of users to a government database in real time – this is unlikely to be necessary and proportionate in the context of a public health response. Technology can play a useful role in contact tracing to contain COVID-19, but privacy must not be another casualty as governments rush to roll out apps."

Mass Surveillance Tools

Contact tracing apps in Bahrain, Kuwait and Norway follow an invasive centralized approach, posing a great threat to privacy. These systems capture location data through GPS and upload this to a central database, tracking the movements of users in real-time. Qatar's "EHTERAZ" app is capable of optionally activating live location tracking of all users or of specific individuals (at the time of writing it remains turned off).

Authorities in all these countries can easily link this sensitive personal information to an individual, as Qatar, Bahrain and Kuwait require users to register with a national ID number, while Norway requires registration with a valid phone number.

Other apps assessed by the Security Lab such as Tunisia's "E7mi", also follow a centralized model, but instead of recording GPS coordinates, they use Bluetooth proximity scanning to monitor contact between users in real time. Qatar's "EHTERAZ" records and uploads Bluetooth contact between users' devices, along with the GPS coordinates of the encounter.

A major security vulnerability was identified in Qatar's EHTERAZ app, which exposed sensitive personal details of more than one million people. This was especially concerning as the app was made mandatory to use on 22 May. The vulnerability was fixed after Amnesty alerted the authorities to the discovery at the end of May. The security flaw would have allowed cyber attackers to access highly sensitive personal information, including the name, national ID, health status and designated confinement location of users.

Tracing apps from countries such as France, Iceland and United Arab Emirates, use a centralized model, but information on contact between devices is uploaded only when users voluntarily decide to report themselves as symptomatic or at the request of the health authorities. Such voluntary and consensual uploads at least reduce the risk of mass surveillance, as data is not automatically uploaded. The centralized model of France's contact-tracing app combined with the lack of transparency over how data is stored raises questions as to whether the users' information could be deanonymized.

"Governments across the world need to press pause on rolling out flawed or excessively intrusive contact tracing apps that fail to protect human rights. If contact tracing apps are to play an effective part in combating COVID-19 people need to have confidence their privacy will be protected," said Claudio Guarnieri.

New forms of surveillance

Bahrain's app was even linked to a national television show called "Are You at Home?", which offered prizes to individuals who stayed at home during Ramadan. Using contact details gathered through the app, 10 phone numbers were randomly selected every day using a computer programme, and those numbers were called live on air to check if the app users were at home. Those who were won a prize. Inclusion in the television programme draw was initially mandatory until Bahrain's Information and eGovernment Authority added an option to its BeAware Bahrain app allowing users to 'opt out' of participating in the television competition. The Bahraini authorities have also published online sensitive personal information of suspected COVID-19 cases, including an individual's health status, nationality, age, gender and travel history.

Both the Bahraini and Kuwaiti apps can pair with a Bluetooth bracelet which is used to make sure the user remains in the vicinity of the phone, in order to enforce quarantine measures. The Kuwait app regularly checks the distance between the Bluetooth bracelet and the device, uploading location data every 10 minutes to a central server.

Location data and additional diagnostic information from the Bluetooth bracelet linked to the BeAware Bahrain app is frequently sent to a central server. It is mandatory for all individuals registered for home quarantine to wear the bracelet and those who do not can face legal penalties under the Public Health Law No. 34 (2018), including imprisonment for at least 3 months and/or a fine of between BD1,000 and BD10,000 (approximately US$2,700, and US$27,000 respectively).

Privacy and human rights by design

Contact tracing is an important component of effective pandemic response, and contact tracing apps have the potential to support this objective. However, 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. Any data collected must remain anonymous, including when combined with other data sets.

"Governments rolling out centralized contact tracing apps with real-time location tracking need to go back to the drawing board. There are better options available that balance the need to trace the spread of the disease without hoovering up sensitive personal information of millions of people," said Claudio Guarnieri.

Notes to editors

For more information or to arrange an interview, please contact: tom.mackey@amnesty.org or press@amnesty.org

Summary of Contact Tracing Apps Analyzed by Amnesty's Security Lab

Amnesty International's research into COVID-19 apps found that apps tend to fall into three categories. Firstly, those that are not in fact doing digital contact tracing but rather allow users to voluntarily record and check their symptoms (e.g. Lebanon and Vietnam).

Secondly, apps which use a much less invasive decentralized model of Bluetooth contact tracing like that developed by Google and Apple. Under this model, data is stored on people's phones, rather than on a centralized database. This includes countries such as Austria, Germany, Ireland, and Switzerland. Amnesty International did not undertake a technical review of any apps that follow this model as they tend to be less concerning from a privacy perspective and are still in the process of being rolled out.

The third, and most serious for human rights are contact tracing apps, which are centralized, meaning they log data captured via the phone's Bluetooth sensor or via GPS (or both) and upload this data to a centralized government database, and in some cases are mandatory. Amnesty International wrote to authorities in Bahrain, Kuwait and Norway before publication to notify them of the privacy and security vulnerabilities related to the apps. As of 11 June, the Norwegian government acknowledged receipt of our letter. Amnesty met with the head of development for the Norwegian 'Smittestopp' app on 10 June.

Other problematic contact tracing apps around the world

Amnesty International focused particularly on apps in Europe, Middle East and North Africa. Research by NGOs and media organizations shows there are other apps and digital platforms in other regions which present serious human rights risks, including in China, Ethiopia and Guatemala.

ENDS