Understanding Aarogya Setu: navigating privacy during a pandemic proves to be tricky

Upasana Sharma *(Carnegie India) writes that Aarogya Setu, India's contact tracing application, raises many privacy concerns. And while making the app open source is the right step in ensuring a transparent framework, there is more work to be done in ensuring increased user security and privacy.*

Many countries have launched contact tracing applications to trace the spread of the coronavirus. The Indian government launched the *Aarogya Setu* application on 02 April 2020. This app was made open-source on 26th May allowing global cybersecurity experts to access the source code and detect existing vulnerabilities in the app. While this is a meaningful step in combating the existing privacy issues in the app, domain experts are now claiming that the public version of the code that has been made available is very different from the one actually being used. This recent discussion on the app gives scope to re-examine the existing problems with the app.

Currently, the app has over 120 million downloads and has been recommended by the central and state governments. In response to privacy concerns, the government established an empowered group on technology and data management to ensure effective operation and implementation of the app. The empowered group published a data sharing protocol called the Aarogya Setu Data Access and Knowledge Sharing Protocol, 2020. This document aims to clarify the mechanisms for collecting, storing and using this data while providing safeguards for the same. However, three significant issues with the app remain even after the release of the protocol.

Date originally posted: 2020-07-02

Permalink: https://blogs.lse.ac.uk/covid19/2020/07/02/understanding-aarogya-setu-privacy-during-the-pandemic-may-be-compromised/

Blog homepage: https://blogs.lse.ac.uk/covid19/

The first issue is that the app collects both Bluetooth data and GPS location data. Collecting location data is largely considered unnecessary by most global standards. This is because Bluetooth data is generally considered a better tool for collecting location data, as it only collects data based on its proximity to other phones that have Bluetooth services enabled. This is in contrast to GPS location data which will allow the government to track a user's precise location leaving them vulnerable to being directly identified. MIT's Technology Review has created an index by collating the major contact tracing apps globally, evaluated them on five different criteria, and given them a rating on 5. They have given the Aarogya Setu app a rating of 2 out of 5 stars. The index reveals that only Bahrain, Norway and Qatar are the three other countries collecting both location and Bluetooth data. The developers have not yet clarified why the app uses both Bluetooth and GPS location data.

The second issue is that the personal information of many users of the app is stored on one server. This design potentially allows the government to not only access but also share personal data of users. Earlier last month, cybersecurity expert Robert Baptise who goes by the name Elliot Alderson on Twitter revealed the same. He was able to hack into the database and access the exact location data of infected patients. He could also modify his location to any city of his choice and set his radius parameter to a 100 km. This is problematic because the role of contact tracing apps is only to enable users to check for any active cases in their vicinity and not access the health information of individuals at such large distances. In a response statement, the Aarogya Setu team denied this claim stating that radius parameters can only take the values of 500 metres, 1km, 2 km, 5km and 10 km. They stated that the app collects the user's location data by design and does not violate user privacy. Elliot clarified that as the government collects the GPS data of users it can still use a process called triangulation to track an individual's exact location. It is crucial for the developers to clarify whether triangulation is indeed possible without the user's permission as it is a serious privacy concern.

The third issue is that the tenth clause in the data sharing protocol states that this protocol will be valid for only 6 months from its date of issue, unless the pandemic continues. This is problematic since the empowered group provide an end date to the protocol, they do not provide a similar end date for the app itself. This creates a situation where the protocol that actually provides the safeguards in protecting user data ceases to exist making the user data significantly more vulnerable. In addition, the clause provides no clarity on whether the user data will be deleted or repurposed post the pandemic. It is important to clarify this clause so that users know that their data is being solely during the pandemic and will not be misused later.

Recently, public and private companies have also mandated the use of the app for their employees. Clearly, this practice is being adopted across industries and sectors. As the country slowly resumes its economic activities, this app continues to be used by the Indian population. It is one important way to ensure that work environments are suitable and safe for the employees resuming work. In this situation, while making the app open source is the right step in ensuring a transparent framework, there is more work to be done in ensuring increased user security and privacy. This is especially important as India does not have a data protection law yet. Working on these issues will increase user trust and encourage faster adoption of the app, leading to better pandemic prevention.

This post represents the views of the author and not those of the COVID-19 blog or LSE.

Date originally posted: 2020-07-02

Permalink: https://blogs.lse.ac.uk/covid19/2020/07/02/understanding-aarogya-setu-privacy-during-the-pandemic-may-be-compromised/

Blog homepage: https://blogs.lse.ac.uk/covid19/