SFLC.IN
K-9, Second Floor, Birbal Road,
Jangpura Extension,
New Delhi-110014
(tel): +91-11-43587126
www.sflc.in

OVERVIEW ON DATA AND PRIVACY CONCERNS DURING THE COVID-19 PANDEMIC

Agenda : Oral Evidence on citizen's security and privacy by the representatives of Ministry of Electronics and Information Technology.

I. PRIVACY CONCERNS

a) Aarogya Setu: The Aarogya Setu has been made open source. Open-sourcing a software ideally involves release of server code, client code, and the cloud and deploy functions which provide for verifiability of server code. As of now, only Android code has been released which has been developed by private sector volunteers without any association clearly stated. The client available via play store is not a verifiable build complied from the public repository. Without server code and client deploy functions, there is no transparency. The current open-sourcing does not help in providing clarity on how the tracking data is controlled.

The Data Access and Knowledge Sharing Protocol provides the option to user to delete its demographic data. However, the App does not provide that option and the MeitY has not clarified if uninstallation amounts to deletion.

Besides, the Aarogya Setu is a centralised application i.e. user's personal information is stored on Government server at the time of registration, if the user has been tested positive, and if reports yellow/orange during the self-assessment test. Most of the proximity tracing applications are decentralised in nature i.e. only the unique ID is uploaded on government server.

b) Broadcast Engineering Consultants Limited (BECIL) Tender: BECIL, a government of India undertaking, has recently released a tender inviting "Expression of Interest (EOI) for Empanelment of Agency for Supply of Healthcare Equipment". To this tender, a corrigendum was released adding 3 more items to be supplied including a **COVID-19 Patient Tracking Tool**. Reading through the specifications of the tracking tool, it is evident that the item, presumably a comprehensive software, goes beyond a healthcare tool and opens up the

possibility of mass surveillance. The tool with analysis of cell tower dumps and gateway scans and call detail records (CDR) has the potential to be used as mass surveillance tool.

c) India Health Stack : The Bharat Health Stack envisioned by the NITI Aayog is in its formative stage. The NITI Aayog has also stated that Aaorgya Setu is the building block of Bharat Health Stack. However, in the absence of privacy laws in India, there is no clarity as to how the health data will be safeguarded and to what extent will it be shared with private companies. Considering that private companies like 1mg, Practo are associated with the development of India Health Stack, it might also lead to conflict of interest.

d) **Data Breach of Customers' with BHIM App:** The vpnMentor's research team recently discovered a breach of sensitive financial data leaking from a website linked to the Bharat Interface for Money (BHIM). The breach was reported to CERT-In and the breach was closed. This could have led to identity theft, tax fraud, theft, and fraud. The source of breach was not the BHIM App itself but a website operated by the Common Service Centres (CSC) which is an undertaking of the MeitY. The forensic analysis of the breach was not shared by the BHIM or the CSC. In fact, the National Payments Corporation of India (NPCI) stated that there has been data compromise. It is estimated that the data of around 70 lakh Indians may have been exposed by the CSC BHIM website.

e) **Technology Development Board Approved Technologies to Augment India's Efforts to Combat COVID-19:** The Technology Development Board (TDB), a statutory body of the Department of Science and Technology (DST). The TDB has approved 6 projects for commercialisation. The equipment approved includes an equipment by Cocoslabs Innovation Solutions Private Limited whose specification includes detection and tracking a person with and without mask, prediction of age, gender, race, temperature readings, and facial recognition in a single product that can track multiple people in a real-time environment. Similarly, Advance Mechanical Services Private Limited is developing an equipment which shall have imaging processing software and AI protocols development. This has the potential to be used as a tool for mass surveillance.

II. SUGGESTED QUESTIONS FOR THE MEITY REPRESENTATIVES

1. Is there a timeline by which the MeitY intends to release the server-side code of Aarogya Setu mobile application?
2. How will an Aarogya Setu user request deletion of its demographic data? Does uninstallation amount to deletion of demographic data? If not, please state the data deletion mechanism.
3. What is the need to upload user's personal data on government servers if the purpose can be served by uploading the unique digital ID (DiD) only?
4. The BECIL tender could potentially serve as a tool for mass surveillance. What is the use of call detail records (CDR), tower data, and geo-location in a patient tracking equipment?
5. If the BECIL is interested in developing a patient tracking equipment, why has it branded the first specification for the equipment as an "intelligence investigation platform and tactical tool to detect, prevent, and investigate threats to national security using CDR, IPDR, Tower, Mobile Phone Forensics Data"?
6. While building the Bharat Health Stack, has the government taken any steps to ensure that the health data of citizens is safeguarded? How were the companies involved in the building of Bharat Health Stack shortlisted?
7. How is Aarogya Setu Mitr portal related to the Aarogya Setu mobile application. The employees of some of the companies listed in this website were involved in the development of Aarogya Setu app. Was there any policy on preventing conflict of interest signed by the volunteers involved in the development of Aarogya Setu app?
8. Is there any protocol on reporting of data breaches in place by the Common Service Centres and the BHIM? If so, what steps are taken after the breach has been reported? What transparency and accountability measures are in place to inform the users registered with the platform?
9. Please state the specifications and features of thermal scanners which are being developed by Cocoslabs. and Advance Mechanical Services Private Limited.

III. REACH OUT TO US

As an organization working extensively on promoting and protecting digital rights of Indian citizens for a decade, we would be honoured to assist you with our research, technology expertise and digital security training sessions, to help the cause of preserving and promoting digital rights and freedoms of citizens.
Please reach out to us at **firm@sflc.in.**

IV. ABOUT US

SFLC.IN is the first Indian legal services organization that works exclusively on technology, law, and policy. As of May 2020, it is the only Indian organization to be inducted as a member of the **IFEX** (International Freedom of Expression and Exchange), a global network to defend the right to freedom of expression and information. In its mission to empower Indian citizens of their digital freedom and rights, it has made numerous representations before various Government departments/ entities and filed litigations before the Hon'ble Supreme Court of India and several High Courts, on Intermediary Liability, Mass-Surveillance, Software Patents, and Internet shutdowns.

SFLC.in promotes innovation and open access to knowledge by helping different stakeholders make informed and just decisions regarding the use and adoption of technology. We make representations in Intellectual Property Rights disputes, equipment technology cases, data protection, and content takedown (Intermediary Liability Disputes).

For more detailed analysis, please refer to our posts on https://www.sflc.in/
For tracking instances of internet shutdowns in India: https://internetshutdowns.in/
For Digital security training: https://security.sflc.in/