Designing new-age Government to Citizens (G2C) applications based on the principles of "Technology as a public good" and a microservices based architecture

Carsten Maple*, Venkat Goli,
Anshul Pachouri, Suhird Singh

*Professor Carsten Maple, Turing Fellow, Professor of Cyber Systems Engineering in WMG at the University of Warwick.

MSC MicroSave Consulting | www.microsave.net

1.0 Background

Over the past five years, India has embarked on a huge transformation in its approach to leveraging technology to connect with its citizens and to deliver public services in an effective and efficient manner. The more prominent use of digital technologies based on digital ID (in the form of *Aadhaar*), to curb leakages in India's public services delivery programs, has been especially seen in public distribution system and social transfers[1].

The successes of the Government of India in implementing a range of digital technology initiatives (such as Digital Locker, e-Sign, UPI, GST etc.) have prompted Indian states to develop and deploy various digital applications to offer public services. Many Indian states have adopted an approach to develop a new mobile application and/or web-portal for every individual department or scheme. This has led to the situation where citizens find themselves **inundated with a plethora of information and a choice of multiple digital applications**. This trend has become more apparent during efforts to address the challenges of the COVID-19 pandemic.

The seventh schedule of the constitution of India lists public health under List-II (State list)[2]. This makes health, sanitation and issues concerning hospitals and dispensaries a state matter, giving states the right to legislate and issue orders on related issues. However, the Epidemic Diseases Act, 1897[3] and the National Disaster Management Act, 2005[4] give powers to the Union Government to take actions during epidemics and national disasters. In fact, both the announcement of a nation-wide lockdown and the subsequent notifications and orders that were issued by the Union Government during the COVID-19 pandemic draw their legitimacy from these two acts. States have complete jurisdiction to launch tools for disseminating information, through means such as mobile applications, in the interest of public safety. It could be argued that a coordinated and planned effort with the Union Government would go a long way to avoiding confusion among the general public.

[1] "Lessons from the Digitisation of Government to Person (G2P) Programmes in India", Microsave Consulting (MSC), June 6, 2018

[2] The Constitution of India has 12 schedules. The seventh schedule deals with the division of power between the Centre (Federal government) and the states. The seventh schedule has three lists – a.) Union List (List I), b.) State List (List II), and c.) Concurrent List (List III)

[3] "The Epidemic Diseases Act, 1897", Ministry of Law and Justice, Government of India

[4] "The Disaster Management Act, 2005", Ministry of Home Affairs, Government of India

2.0 Development of mobile apps to address COVID-19 pandemic by Indian states

With the commoditization of mobile application development and the availability of tools to automate the process of writing application programming code, the time taken to create mobile applications, and the associated complexities involved in creating them, have been significantly reduced. This has worked well for government bodies that wanted to create tangible and observable interventions to address the issues arising from the COVID-19 pandemic. As a result, various state governments have created their own mobile applications as a demonstration of their proactivity and performance.

As the pandemic progressed, states - and even districts within states - started to create bespoke (yet ultimately very similar) mobile applications to differentiate themselves from their peers. Such action was well-received and perceived as a strong pro-active initiative by sections of the population that were digitally empowered. Since such groups can be more vocal on a variety of platforms, including social media, it resulted in creating a 'positive buzz' for the state/entity that created the mobile application, further incentivizing such behavior.

The creation of these mobile applications has further accentuated, in some ways, the issue of exclusion and limited availability of information for those that are digitally excluded. While the creation of mobile applications makes information readily available to those with the technology to access it, it does not solve the problem for those digitally excluded individuals and communities. This includes those with feature phones that have no internet and those with no mobile phone at all. To ensure that the digitally restricted have access to the same information as the digitally empowered, governments can set-up functional help-lines, auto-dialers, Short Messaging Service (SMS) text messages, and other channels that provide these groups with the same information. Governments that are not making adequate investments in these channels, on the pretext of the wider reach of digital applications, face the risk of their digitally limited citizens relying on unverified news and falling prey to disinformation. Hence, it could lead to a situation where those who are most vulnerable to the pandemic are left without access to first-hand information for a sustained period of time.

Since the announcement of the first lockdown on March 24, 2020, at least 35 mobile apps specifically addressing COVID-19 were developed by 25 states and Union Territories (UTs) of India. As of August 11, 2020, 27 mobile apps of these mobile apps provided general information on the COVID-19 and 7 apps allow tracking of nearby COVID-19 cases. Of all the mobile apps, 15 have a quarantine tracking feature and at least 4 of these mobile apps required prior registration with the state health department. Consideration of the 35 mobile applications revealed that 17 mobile apps provide

information on COVID-19 hospitals while only 3 apps provided information on isolation beds. Some of the mobile apps also facilitated the home delivery of essential items (grocery, medicines etc.) and 7 provided the means for application of mobility passes.

It is clear that the mobile applications developed have not benefitted from standardization of information and a coordinated development approach. Analysis shows that there is no consistency in features, functionalities and regularity of information updates in the various mobile apps on COVID-19 operated by the different state governments. The principle of having a primary unit of data entered only once and then using Application Programming Interfaces (APIs), or similar architectural frameworks, for systems to share data has long been established. However, it would appear that such practices have not been used in the development of the majority of the mobile applications. This has resulted in data being updated manually in the mobile applications, leading to a lack of single source of truth and time-lags in data-flow from hospitals to the state headquarters. The slow pace of data refresh has in turn led to a false sense of security amongst users, since they do not have access to the latest data, leading them to think they are safer than they may be in reality.

The majority of these state mobile apps also differ significantly on the data-privacy provided, depending on the information/permissions they request the user for operating them. We observed that 31 of the 35 mobile apps request access to location services, 9 mobile apps request access to device ID and call information, 5 mobile apps request access to Bluetooth settings, 15 mobile apps request access to the camera, 3 mobile apps request access to contact information, and 3 mobile apps even request for access to the user accounts on the device. It seems that these data requests may not meet the two established principles of data privacy i.e. necessity (is the data necessary for the mobile application to achieve its goal) and proportionality (is the collection of data proportionate to the extent to which an individual's right to privacy is being infringed). The mobile applications developed could have proactively followed agreed principles of privacy by design, such as minimal data collection and end to end data security.

In addition to the state-driven efforts, the Government of India is also running its flagship mobile app Aarogya Setu to spread awareness on COVID-19, to track the COVID-19 cases in any area, and to direct people to the appropriate health services. The mobile app also tracks the spread of COVID-19 through the use of GPS and Bluetooth features in smartphones.

3.0 Advantages of a microservices based framework

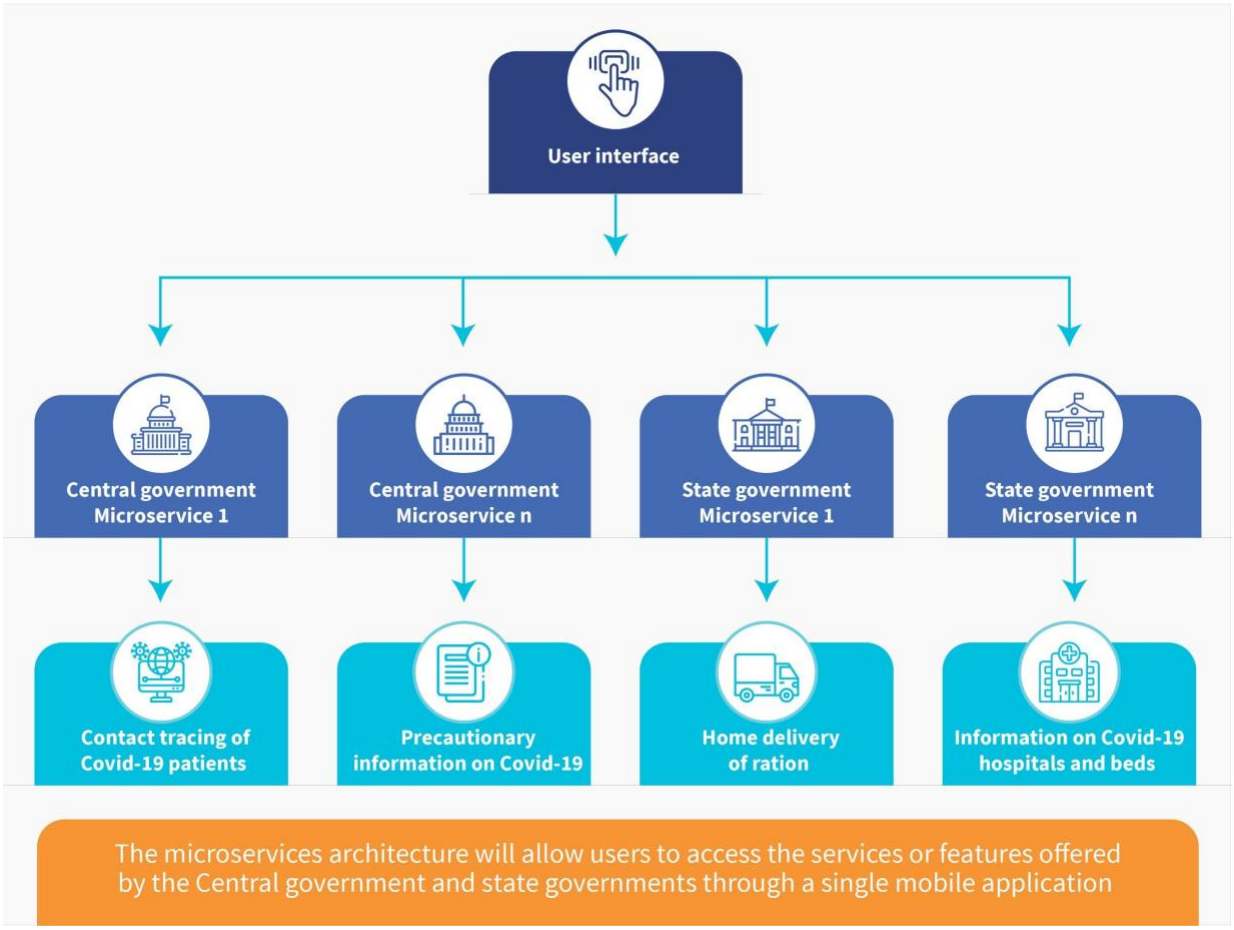
The redundant features of numerous states mobile apps on COVID-19, duplication of efforts, non-uniformity in data-privacy, and confusion among end users point towards the larger need for an open, interoperable, API-based microservices architecture that can integrate (or host) the state digital applications with the central government's application. The adoption of an API-based microservices architecture and federated database structure, with an appropriate governance framework, could address these issues by allowing Aarogya Setu to be integrated with the myriad of multilingual state mobile apps to offer both its standard services (contact tracing, real-time information on cases) and state-specific customized services or sub-applications (such as information on hospital beds, grocery shops and so forth).

The ongoing implementations of the Corona Safe Network in Kerala and the Uniform Data Platform of Uttar Pradesh offer some useful perspectives in this regard. The Corona Safe Network is an open-source public platform that brings together innovators and volunteers to support the Government of Kerala in its ongoing battle with the COVID-19 pandemic. The open-source platform has been used to develop, test, and deploy multiple applications on contact tracing, telemedicine, availability of hospital beds and quarantine facilities, and ambulance services, among others. The Unified Data Platform in Uttar Pradesh facilitates a singular point of data input (case registration) and integrated work-flow based system leading to a single source of truth and effective data management throughout the COVID-19 case life-cycle. The platform integrates the data from multiple sources such as call centers, testing labs, self-quarantine apps, and hospital case-load to provide a singular and integrated view of the COVID-19 situation in the state. It also assists in prompt decision-making using advanced analytics to identify spread patterns and clusters of high-infection.

Adopting the similar principles of 'technology as a public good', a common platform could be developed to bring all the state governments together around a common set of critical features of a digital application (common digital applications having different sub-applications encompassed for various states and union territories) on COVID-19 enabling state-specific features/sub-applications to be added to the common digital application at a later stage. The development of critical features could then be managed by the central government while the design and development of sub-applications/state-specific features could be undertaken by the respective state governments.

The API-based microservices architecture would also allow the integration of state-specific features in a common digital application without any interference from other sub-applications. The principles of a federated data structure would allow common digital applications to virtually access databases of various states and UTs depending on the location/state of the user without making any compromise on data-security and sovereignty issues. In comparison to the conventional method of developing digital and mobile apps, a federated, microservices-based approach could also offer more flexibility to the user to share its information since the data is not uploaded to a central server, but rather is stored locally on users' devices.

Figure 1: Proposed microservices architecture of the Covid-19/government mobile apps



As such, a common digital application (based on interoperable, open, APIs based federated microservices architecture) could offer a mix of common plus differentiated services to all its citizens (based on geography) while maintaining a higher degree of standardization and predictability. This approach would fundamentally change the way G2C services are currently delivered in India and would bring significant cost-efficiency, synergy, standardization, and agility in the public IT systems. Of course, it is vital that an appropriate and robust governance framework is established to oversee access to the data.

4.0 Decentralized information-flow as a next step

Many countries in Europe have considered moving from an information flow that is centralized to a decentralized information flow for contact tracing applications. This was largely driven by concerns regarding privacy, as centralized databases can have a higher risk of data leaks and security breaches. Also, a decentralized information flow, owing to information residing in many individual systems and not in a centralized system, increases the cost while reducing the reward of effecting a successful

breach. This led to Germany[5] adopting a decentralized information flow for their contact-tracing application and the majority of other countries following suit.

In the case of a centralized approach, proximity data must be stored and processed on a central server controlled by a national authority. The increased health authority verification that is provided by this approach comes at the cost of citizens providing information upfront, which may lead to a compromise in their privacy, as well as less finely-grained control.

Conversely, in a decentralized information-flow approach, contact data is not uploaded to a central server, and can be stored locally on user's devices, with uploading of data taking place only under certain circumstances, such as a confirmed COVID-19 diagnosis. In the case that data is not uploaded to third parties, a decentralized information-flow approach would offer privacy benefits over a centralized approach. It is recognized, however, that this requires marginally more computing power on the client side.

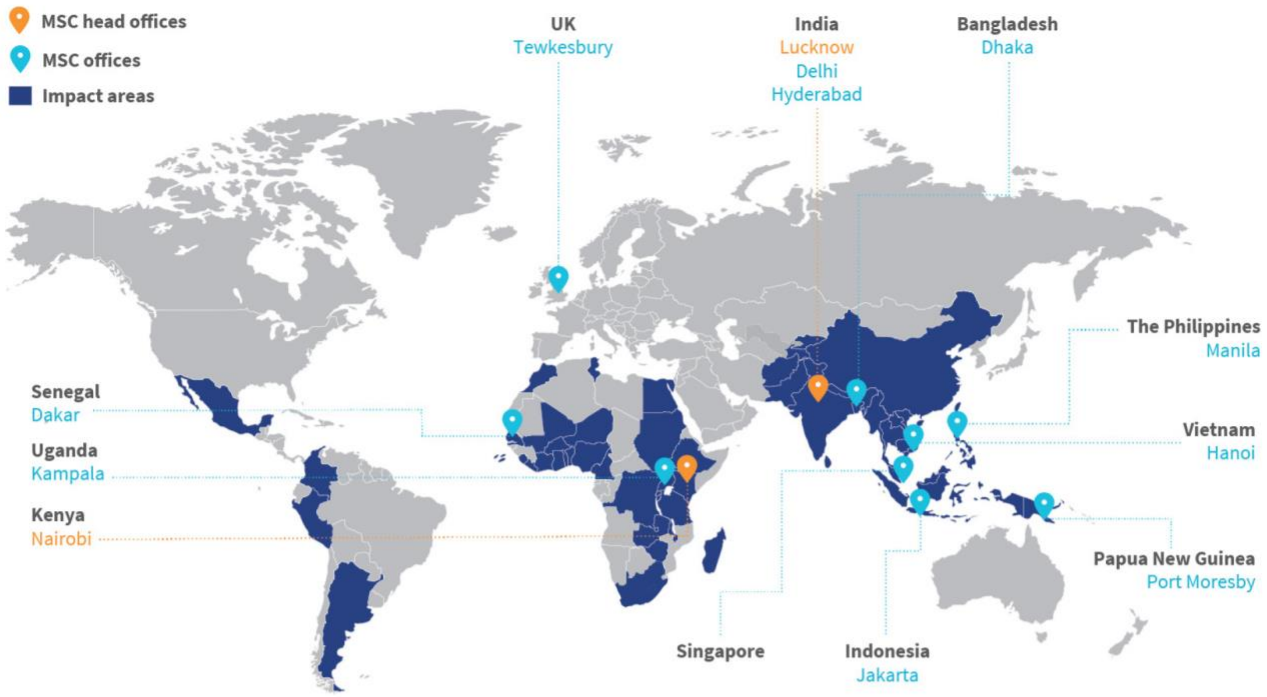
The apps that have been developed by various states and union territories of India in the analysis employed a centralized approach, which has a higher risk of privacy compromise. In the future, design considerations for these apps should evaluate the need for a centralized approach and whether the same goals can be achieved through a decentralized information-flow. While this may not be an immediate goal, a long-term decentralized application architecture would go a long way in further preempting some of the issues of data privacy and ownership.

****

Appendix 1: Mobile applications developed by Indian states to address Covid-19 pandemic

[5] "Germany flips to Apple-Google approach on smartphone contact tracing", The Reuters, April 26, 2020

MSC
MicroSave Consulting



Asia head office

28/35, Ground Floor, Princeton Business Park, 16 Ashok Marg,
Lucknow, Uttar Pradesh, India 226001
Tel : +91-522-228-8783 | Fax : +91-522-406-3773
Email : manoj@microsave.net

Africa head office

Shelter Afrique House, Mamlaka Road, P.O. Box 76436,
Yaya 00508, Nairobi, Kenya
Tel : +25-420-272-4801 | Fax : +25-420-272-0133
Email : anup@microsave.net

www.microsave.net