Source: *The Straits Times,* pA18
Date: 13 June 2020

Getting buy-in for TraceTogether device and future Smart Nation initiatives

Set up an independent body to vet transparency and have a citizens' panel to develop principles for privacy and use of personal data

Carol Soon

For The Straits Times

In the past week, the Government announced its plan to roll out a wearable contact tracing device to help curb the spread of Covid-19.

Public backlash against the TraceTogether Token initiative was swift. Within a short span of three days, a petition against the development of the device attracted about 30,000 signatories.

The Government has since clarified the key features of the device to address people's concerns – it will not track a person's location, and will be small enough for people to put into their bags or pockets. Those who prefer to use the TraceTogether phone application can continue to do so.

While the Government can provide assurances and citizens can make compromises, the tension between the need to gather personal data for the collective interest and people's desire to protect their privacy is a perennial one.

Although the TraceTogether app and wearable device are designed specifically to allay fears of surveillance overreach, people's wariness and suspicions pertaining to any attempt to monitor their movements are unlikely to go away.

Public sensitivity to surveillance has increased over the years, amid the Cambridge Analytica case, racial profiling in the West, and local security breaches and data leaks.

Therein lies the dilemma. This hypersensitivity brushes up against the need for personal data to be shared for the public good, especially in national crises.

Without widespread voluntary adoption, the efficacy of contact tracing devices will be low. And it is very likely that people will need to give up even more personal data in the future to be ready for the next pandemic or national emergency.

So what is the solution in a new post-Covid-19 normal? Transparency, trust and collaboration.

TRANSPARENCY: AN INDEPENDENT BODY

First, the Government must be transparent and communicate all measures as well as their attendant benefits clearly.

Most people have few qualms about submitting their personal information to a wide array of businesses, such as social media platforms, fast-moving consumer goods businesses, e-commerce and peer-to-peer sharing platforms.

For most people, willingness to give up their personal data depends on what they are getting in return for surrendering it.

A Pew Research Centre study in 2016 found that many Americans said their sharing of personal information was contingent on the benefits they received and how much risk they faced.

For instance, almost half said the benefits they received from retail loyalty cards justified stores' tracking of their purchases.

A Cisco study conducted last year on more than 2,600 adults worldwide found that about one-third of the respondents were "privacy actives" – people who take actions such as switching service providers because of the companies' data policies.

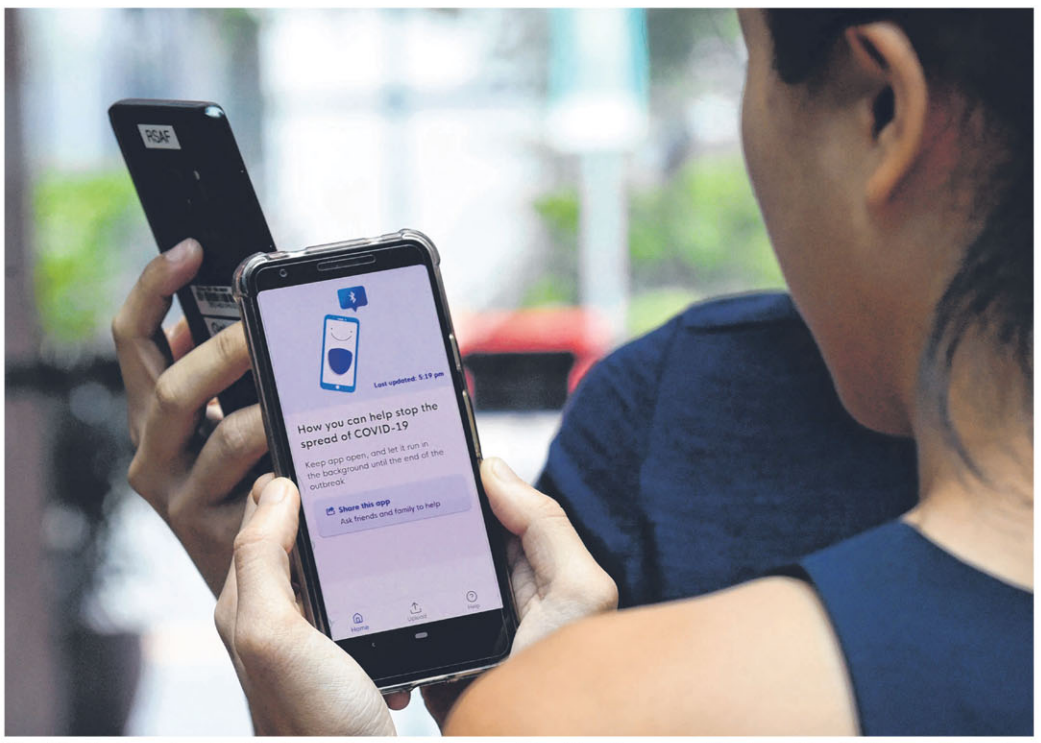
Interestingly, this group is comfortable with trade-offs such as providing their purchase history in exchange for personalised products and services, and sharing information from smart home speakers in exchange for health and safety warnings for the entire family.

In Singapore, too, people can be expected to make trade-offs between privacy and convenience, as seen in the general acceptance of Smart Nation initiatives to better meet Singaporeans' living, transport and health needs.

In Yuhua estate, one of the first Housing Board towns to "go smart", sensors are installed in flats to measure energy consumption, waste production and water use in real time.

Both parties benefit – the Government has access to data that helps it improve the planning, design and maintenance of public housing estates, and residents receive feedback nudging them to adopt more environmentally friendly habits, which in turn reduces household costs.

The Elderly Monitoring System, another Smart Nation initiative, uses sensors on doors and inside rooms to monitor the movements of seniors. Such a move could be perceived as highly intrusive. But the use and benefits are clear – the system will help to alert caregivers when no activity is detected.



The effectiveness of contact tracing technology such as the TraceTogether app will be low without widespread voluntary adoption, says the writer. Collaboration between citizens and the Government is key. PHOTO: AGENCE FRANCE-PRESSE

One way to assure citizens of the Government's commitment to transparency is to set up an independent body that oversees the use, effectiveness and privacy protections of any technology that is designed to solve exigencies faced by the country.

Such a move was proposed in the United Kingdom in response to the National Health System's move to roll out a contact tracing app.

The independent body could also deal with complaints from the public and ensure that technology developers – government and non-government – meet key requirements.

These could include a declaration of the limitations of the technology and clear stipulation of how long the data will be kept, as well as the criteria that public agencies have to meet to use the technology.

TRUST: NEGATIVE AND POSITIVE LISTS OF ACTIONS

Second, transparency is futile in the absence of trust.

Here, some lessons can be learnt from South Korea. The country has been regarded as a model for the use of electronic surveillance, which has enabled it to avoid severe lockdowns during the pandemic.

In times of emergency, its infectious diseases Act is invoked to do large-scale contact tracing involving multiple data points – citizens' mobile phone location records and credit card transactions, closed-circuit television footage, and the global positioning system.

The Act, which accords infectious diseases investigators access to personal data, was created after the Middle East respiratory syndrome outbreak in 2015, when South Korea suffered the largest number of infections outside the Middle East.

Coupled with the exemption from the Personal Information Protection Act for public interest purposes, such as for infectious diseases investigations, the Act allows the authorities to identify and isolate potential Covid-19 cases rapidly.

Publicly sharing confirmed patients' movement history enables other citizens to stay vigilant and protect themselves from exposure to the disease.

While South Koreans largely understand and accept the use of the Act, concerns were raised when a recent outbreak in an area of the Itaewon nightlife district where there were gay clubs inadvertently outed some people.

To mitigate such risks, Associate Professor Sonn Jung Won from University College London proposed at a recent Institute of Policy Studies (IPS) online forum on data privacy the creation of "positive" and "negative" lists.

The first will clearly state the different types of data that the Government can have access to, and in what situations.

Currently, the Korea Centres for Disease Control and Prevention must go through the police to access citizens' mobile phone and credit card data.

However, not everyone is comfortable with having their identities revealed, such as members of the LGBTQ (lesbian, gay, bisexual, transgender and queer) community.

Thus, the need for a "negative" list stipulating what the Government is not allowed to do with the data collected.

COLLABORATION: A CITIZENS' PANEL

This leads to the third crucial factor – collaboration. Given that the efficacy of government efforts resides in citizens' support and buy-in, the Government and citizens need to work together to come up with a sustainable approach to solving the conundrum.

My colleague, Mr Christopher Gee, at the IPS online forum, mooted the idea of a citizens' charter where Singaporeans decide on the guiding principles regarding private and public data, and how they should be used. This can be done by convening a citizens' panel, where people from different backgrounds come together and decide as a collective what goes into the charter.

Having worked with various government agencies on such panels, I have seen first-hand the positive impact the process has had on policymaking and citizens' lives.

When exposed to the different lived realities of others, people are forced out of their comfort zones to confront and address preconceived notions.

The deliberative process of a citizens' panel is designed to elicit diverse views and guide informed collective decision-making.

The Government can then take on board the people's recommendations and develop a model that governs the use of citizens' data, one that could well be uniquely Singaporean.

While the present dangers of Covid-19 demand urgent measures, a citizens' panel is a good idea going forward, given that many Smart Nation initiatives and intrusive devices are being planned.

Singapore needs to address these three factors urgently to achieve a working compromise between personal data and public good. If not, misunderstandings and resistance will continue.

We should try to resolve this before the next pandemic or national emergency hits.

stopinion@sph.com.sg

• Dr Carol Soon is senior research fellow and head of the Society and Culture Department at the Institute of Policy Studies, National University of Singapore.