RSIS S. RAJARATNAM SCHOOL OF INTERNATIONAL STUDIES
Nanyang Technological University, Singapore

RSIS COMMENTARY

www.rsis.edu.sg No. 018 – 2 February 2021

Smart Nation: Privacy Protection and Public Trust

By Teo Yi-Ling and Manoj Harjani

SYNOPSIS

An unexpected U-turn by the Singapore government on its initial undertaking that TraceTogether data would only be used for COVID-19 contact tracing purposes wrought strong reactions from the Singapore public. What does this portend for public trust in future Smart Nation initiatives?

COMMENTARY

IN THE course of implementing TraceTogether – a digital system to facilitate contact tracing efforts in response to the COVID-19 pandemic – assurance had been given at the highest levels that individual privacy would be respected. Accusations have, however, been levelled at the government of breaking trust and leveraging technology for political control. Legitimate questions have been asked about when it knew that existing Criminal Procedure Code provisions covered use of TraceTogether data, and why disclosure of this fact was not made upfront.

Privacy lacks a clear definition in the Singapore context – does it refer to privacy of the person, their data, or both? There is no black-letter law in Singapore enshrining privacy of the person – it is not a constitutionally-guaranteed right. Where the Personal Data Protection Act (PDPA) is concerned, it only provides for the obligations of businesses in protecting customers' personal data and does not cover government use of personal data. What impact will this controversy have on public attitudes towards adopting future data-driven Smart Nation initiatives?

Respecting Privacy

The Singapore government's inexorable march towards a Smart Nation has thus far been presented as a *fait accompli*. However, there is now a clear and urgent need to

reconsider the current approach, particularly given broader shifts that have been unfolding in the public trust environment in Singapore.

Automation and digitalisation have provided considerable convenience at work and in daily life. The trade-off for accessing this convenience is providing personal data and private information. Yet confidentiality and privacy cannot be guaranteed as companies and government agencies can tap into data repositories for all kinds of reasons. How might individuals safely navigate this trade-off in a digital existence without losing what they hold dear and personal, and who can they trust to guide them?

The Singapore government has previously acknowledged the negative impact of distrust upon Smart Nation efforts. Before pressing on with more Smart Nation rollouts, it is then crucial to strengthen public trust by addressing two immediate matters.

The first is creating a clear definition of privacy. The second is publicly clarifying the government's guiding principles regarding decision-making involving personal data. These will allow the public to understand what is at stake.

How the government responds to the TraceTogether controversy will determine whether Singapore can manage the growing global concern regarding smart city endeavours – erosion of personal privacy and liberty in the name of public safety and efficient service delivery.

Coherency, Transparency and Accountability

The PDPA's current focus is on how businesses manage personal data – there seems to be an assumption that if businesses are regulated, citizens' interests will be protected by proxy. This is risky given continuing data breaches and growing concern about misaligned incentives for Internet companies that profit directly from personal data.

Exacerbating the situation further is the government's exemption from the PDPA despite it being the most significant user of data in Singapore and occasional lapses in data security management by government agencies.

An uncomfortable precedent appears to have been set regarding repurposing data gathered ostensibly in the public interest for law enforcement and regulating individual behaviour. To be sure, the issue is far less about data being accessed by law enforcement agencies, than it is about the relative ease with which the original limits on the data's use were lifted.

Given the breadth of the multi-agency taskforce leading Singapore's pandemic response, it is not easy for some citizens to accept the government's explanation that it did not anticipate potential use of TraceTogether data for investigative purposes, and why it did not proactively address this publicly upon realisation.

Improving Governance of Data-related Issues

Nevertheless, there is a clear imperative emerging from this controversy to improve

governance of data-related issues. The Government Data Strategy formulated in 2018 already lays out a sound approach for the public sector to better leverage data; the Public Sector Data Security Review in 2019 complemented this with recommendations to improve data security.

What is missing, however, is clarity on accountability for use of data by the government beyond ensuring its security.

To address this, the government should consider developing a broader framework for data governance and implement it in a transparent manner so the public is aware of the "who, what, when, where, why and how" when it comes to their personal data.

This way, the government will by design be able to account for how it collects and uses data – ideally in a manner that the public can digest at every touchpoint where their personal data comes into play.

Beyond data, the government will also need to address a current lack of regulations governing its development and adoption of digital technologies in an ethical manner and in the public interest. To this end, the government should consider creating an ombudsman for ethical development and deployment of technology, with a complementary audit process subject to transparency in the public domain.

Road Ahead: Need for National Conversation

On the broader issues of privacy regulation and rights, change may be on the horizon. In December 2020, the Law Reform Committee issued a report proposing a new law addressing insufficiencies and incoherencies in the current patchwork of privacy legislation.

To what extent this proposed law impacts Singapore's Smart Nation agenda is yet to be seen, but it is being surfaced at a time when the national discourse on privacy is sharpening. This is a critical opportunity for a meaningful and open public conversation.

Singapore has busied itself with the legislative infrastructure to speed up the drive towards Smart Nation-hood, but has spent less effort on the contentious issue of how individual rights will be affected by digitalisation, and what the public really wants – or needs – out of the government's adoption of technology.

As we progress towards becoming a Smart Nation, we must now reckon with a renegotiation of the social contract and legitimate expectations on both sides – the more digitally transformed our lives become, the more we must remember our humanity, values, and vulnerabilities.

Teo Yi-Ling is a Senior Fellow and Manoj Harjani is a Research Fellow with the Centre of Excellence for National Security (CENS) and Future Issues and Technology (FIT) Cluster, S. Rajaratnam School of International Studies (RSIS), Nanyang Technological University (NTU), Singapore.

Nanyang Technological University
Block S4, Level B3, 50 Nanyang Avenue, Singapore 639798
Tel: +65 6790 6982 | Fax: +65 6794 0617 | www.rsis.edu.sg