



Trust and consistency go hand-in-hand. Trust is developed when people perceive a pattern of consistency between word and deed.  
BT FILE PHOTO

# Of TraceTogether and trust together

Contact tracing for the sake of public health has a long and storied history, raising moral questions aplenty. **BY DAVID DE CRÉMER, MAHAK NAGPAL AND DEVESH NARAYANAN**

**T**RUST is essential for contact tracing efforts to be successful. However, the recent revelation that Singapore's contact tracing data is available to law enforcement for criminal investigations, in spite of previous reassurances that this would not be the case, has drawn attention not only locally but also internationally. Will the alarm and emergent mistrust pose difficulties for Singapore's fight against the ongoing pandemic?

It is important to situate these worries in historical context. Contact tracing for the sake of public health has a long and storied history, raising moral questions aplenty. Disadvantaged communities around the world, in particular, have long been suspicious that contact tracing efforts might perpetuate – and mask – further discrimination and exploitation.

Take, for instance, contact tracing efforts in the United States in the 1980s, during the early years of the Aids epidemic. At a time when homosexuality was still illegal in many states, compiling lists of gay men and their sexual partners – who were believed to be the source of the epidemic – felt risky and stigmatising. Even as public officials argued that Aids patients had a moral duty to disclose their sexual history, there was widespread distrust that a public health issue was being used to cover and justify discrimination against the gay community.

Optimists might say that as a global society we have learnt from these past mistakes, and that the art of trust-building would be mastered in contemporary contact tracing efforts. However, the recent situation with TraceTogether shows that this might not be the case. It is, of course, reassuring that the Singapore government is listening to concerned voices – issuing a *mea culpa* acknowledging their mistake, and a series of clarifications about the use of TraceTogether data.

## PERCEPTION IS REALITY

However, even as local officials navigate the situation, we see two important caveats in how trust in the TraceTogether app has been approached. Those caveats need to be identified to ensure that the violated trust of many citizens can be successfully repaired. In doing so we rely on decades of behavioral research that has identified one crucial assumption that any trust-building effort has to work with: Trust is in the eye of the beholder.

This assumption suggests that it is not the developer or government that determines the level of trust in the TraceTogether app, but that it is the user who decides whether they perceive

the app as trustworthy or not. And it is in this perception process that we see problems so far:

First, the government's approach to build trust was, and continues to be, to point to certain technical features of the TraceTogether app and token, and label them as trustworthy. Earlier last year, experts were brought in to inspect the TraceTogether token and attest to its privacy-preserving features. And, in response to the backlash after the recent announcement, public officials insisted that citizens could easily write in to delete their stored TraceTogether data.

While this is an empirically-backed approach in order to build community trust, it breaks down in this particular context because of the fact that user trust in contact tracing technology is not determined based on its privacy-preserving features. Rather, users assign trustworthiness to a piece of technology by assessing the trustworthiness of the creator – or the government in this case. In other words, technology has no intentions, but the person (or government) that creates the technology does. If the creator of the technology is worthy of trust, the technology is too.

Second, trust and consistency go hand-in-hand. Trust is developed when people perceive a pattern of consistency between word and deed. So, walk the talk – because ensuring alignment between talk and action is essential in order to reduce the need for coercive state imposition. Inconsistencies between word and deed not only make people doubt your actions and decisions – challenging your perceived integrity – but may also cast doubt on your competence. Much has been said, for instance, about how the public was earlier assured that Trace Together data would be used only for contact tracing, only to now learn that this data could, in fact, be used for certain criminal investigations.

Further, insisting that TraceTogether data is necessary for criminal investigations also seems inconsistent – given the expectation that the use of TraceTogether is temporary, and would no longer be necessary once the pandemic abates. Elsewhere, legal approaches have been used to strictly delimit the use of contact tracing data for the pandemic. In New York, for example, a bill was recently signed into law that protects the confidentiality of contact tracing information.

With those two points, it is easy to understand where things went wrong early on. To begin with, there was an over-reliance on the idea that an emphasis on the technical features of the contact tracing app can help induce trust in users. This, combined with a perceived lack of consistency between word and deed, resulted

in uncertainty about the real intent of the technology. Ultimately, these violations of trust perceptions harm the efficient use of the app and in turn, contact tracing efforts.

Unfortunately, a consequence of these short-term user perceptions is that it is now also likely that any future effort by the government in this area will continue to be viewed in light of the recent violations of trust.

## CLEAR INTENTIONS

Our own research on what it takes to repair trust may help in offering some advice on how to move on now that the damage is done. Citizens want to see what they can expect from the government in the future. In this process it is crucial that the government succeeds in communicating that no bad intentions were involved, and that they do possess the competence to improve the use of TraceTogether. The first lesson to be learnt is thus clearly that any kind of denial will not help in this case. The government should accept that some citizens would have doubts and distrust about TraceTogether, and ensure that their concerns are addressed.

Promises alone, however, will not do the job. Solutions will need to be offered and explained in detail – not only to improve the employment of the app, but also to help rebuild the citizens' trust. And, finally, it is important to ensure that these solutions are acted on in a consistent manner. It is encouraging to already see a few acknowledgements of error, and the beginnings of legal interventions that delimit the use of TraceTogether data.

However, as active debate continues – both in Parliament and the digital public sphere – more concerns and points of distrust may well surface. It is therefore vital that trust is quickly and effectively addressed in the ways we have suggested, so TraceTogether can serve a meaningful and long-lasting role in Singapore's fight against Covid-19.

**■ The writers are from the National University of Singapore's (NUS) Centre on AI Technology for Humankind (AiTH).**

David De Cremer is director and founder of the Centre. He is also a provost chair and professor of management and organisation at the NUS Business School.

Mahak Nagpal is a postdoctoral research associate at the AiTH Centre.

Devesh Narayanan is a research assistant at the Centre, and an MA student with the department of philosophy at NUS.

The opinions expressed are the writers' and do not represent the views and opinions of NUS.