Contact tracing and the data privacy challenge

By Shuman Ghosemajumder

19 Jun 2020

Recent years have seen a marked shift in the way technology interacts with our data privacy. As people live and work in an increasingly digital world, they are also becoming more aware of the information they share and the value of their personal data.

Shuman Ghosemajumder, Global Head of Artificial Intelligence at F5 Networks.

Some regulators have adapted accordingly, with recent legislative examples including the EU's General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA).

Unfortunately, a growing consensus to better protect citizens data now faces one of its greatest challenges yet. As Covid-19 continues to disrupt, governments have been scrambling for technological solutions to model the virus and protect people from infection.

Across the world, this has led to the introduction of contact tracing apps and plenty of associated questions.

First and foremost, how can governments use technology to ensure public health without impacting on personal privacy? And, perhaps most importantly, how can they reassure people that powers used in an emergency will not be leveraged when relative normality returns?

A delicate balancing act

A pressing concern for privacy campaigners is the potential for governments to access mobile phone location data without user consent, even when the pandemic is under control. Other commentators wonder how programs relying on an opt-in method for participation can succeed at scale.

The divide between those favouring centralised solutions (where data is shared with government servers), and decentralised alternatives (where it remains on individual phones), has certainly scuppered any plans for a single contact tracing standard.

Google and Apple recently proposed an option somewhere in between, seeking to build new capabilities into their mobile operating systems that can enable close proximity contact tracing with a degree of anonymisation. The focus is more on the relative proximity between mobile users rather than the absolute location data.

Fans of the approach believe it offers the right balance between tracking movements and identifying infection risk, without creating a store of personal data that could be used for other purposes (or potentially hacked).

At this moment in time, it appears there is no perfect way ahead and more evidence is needed.

Nevertheless, Covid-19 has shown that there is a notable lack of dialogue about the role of technology in shaping public policy. It is a problematic disconnect and one that continues to drive suspicion and mistrust. Moving forward, more governments need to address these concerns head-on, while also acknowledging that these are extraordinary circumstances and should be treated as such.

The big question is how to best leverage technology while also avoiding the downsides of eroding data privacy controls?

One option could be to explore a system similar to Toyota’s famous andon cord.

When a problem arose in a Toyota factory, employees were empowered to halt the assembly line the moment they spotted it. This was achieved by pulling the andon cord so that everyone could quickly align to solve the issue, establish formalised steps to deal with it and then restart production.

A similar system – in other words, an andon cord for data usage – could apply to a situation like Covid-19, provided it includes the following components:

1. **A point of instigation**. The protocol should indicate factors for determining catastrophe on a spectrum. For example, the highest level would be if the continuation of our species is at risk.

2. **A point of demarcation**. Privacy limits need to be reimposed after de-escalation. These should be established with an actual date and time at the outset of the andon cord pull.

3. **A point of privacy**. Wherever additional data is collected, it should be done in a privacy-preserving fashion if possible. For example, MIT's Private Kit is a contact-tracing app that allows infected persons to share their location trail with health officials. The information is anonymised, and patient data is stored locally.

Fundamentally, governments need to accept that they must continually earn trust when it comes to handling data. That means having a bias towards privacy, with clear and transparent parameters that set the terms of how and when to go further. Without transparency, there will be a backlash.

In a worst-case scenario, that could result in individuals undermining public health efforts by disengaging and/or actively seeking to block their devices.

ABOUT THE AUTHOR

Shuman Ghosemajumder, Global Head of Artificial Intelligence at F5 Networks.