Institute of Policy Studies

Report on IPS Online Forum: Private Data, Public Good?

13 May 2020

By Nandhini Bala Krishnan

Published: Friday, 19 June 2020

IPS ONLINE: PRIVATE DATA, PUBLIC GOOD?
IPS Institute of Policy Studies
ONLINE
Dr. Carol Soon
Senior Research Fellow & Head of Society and Culture
Institute of Policy Studies
Assoc. Prof. Jung Won Sonn
The Bartlett School of Planning, Faculty of the Built Environment
University College London
Ms. Teo Yi-Ling
Senior Fellow, Centre of Excellence for National Security
S. Rajaratnam School of International Studies
Mr. Christopher Gee
Senior Research Fellow & Head of Governance & Economy
Institute of Policy Studies

Clockwise from top left: Dr Carol Soon, Associate Professor Jung Won Sonn, Ms Teo Yi-Ling and Mr Christopher Gee discussing the use of contact-tracing apps in Singapore and South Korea

Background

The second part of the IPS Online Forum series, titled "Private Data, Public Good?" was held on 13 May 2020. The 60-minute forum focused on the topic of contact-tracing apps, which have been developed by many countries, including Singapore, as part of their digital surveillance measures to manage the COVID-19 pandemic. The forum aimed to identify some of the existing concerns over the sharing of personal data gathered through such apps, offer possible solutions to overcome them, and examine the implications of sharing personal data beyond the pandemic.

Dr Carol Soon, Senior Research Fellow at the Institute of Policy Studies (IPS) and moderator for the forum, said countries such as China and South Korea were leveraging citizen surveillance to manage the spread of COVID-19. In March, the Singapore government launched TraceTogether, but as of early May only about 25 per cent of the population had downloaded the app. There has been much debate on the use of contact-tracing apps in countries that are rolling out similar initiatives. While the focus has been on the use of personal data during a pandemic, such use of personal data for public good has broad and long-term implications beyond COVID-19.

The South Korean model of electronic surveillance

Associate Professor Jung Won Sonn from the Bartlett School of Planning, Faculty of the Built Environment, University College London, shared how the personal data of citizens have been collected in South Korea and the difficulties faced by the authorities pertaining to what some observers have called, the "overexposure" of people's personal data. He explained that the South Korean authorities have primarily relied on data generated from mobile phone locations, credit card transactions and transportation cards of its citizens. He said contact-tracing apps in South Korea have been used to trace the locations of confirmed patients and those who had been in close contact with them. The apps have not been used to find new patients.

However, there have been some privacy concerns with regard to the gathering of personal data by certain segments of the society. On 6 May, it was discovered that a person who later tested positive for COVID-19 had visited five separate nightclubs in one evening, causing them to become virus hotspots. These declared hotspots were located within areas where the LGBTQ community was known to frequently gather. Some members who had visited these hotspots were reluctant to come forward for testing as they were concerned that their identities would be revealed. To manage this, the government used information generated from mobile phone locations of over 2,000 members who visited the hotspots on the day to help in their contact tracing. The government also promised complete anonymity to encourage more members to come forward for testing. In the event of non-cooperation, the government also resorted to imposing fines up to US$2,000. On its part, some members of the LGBTQ community collaborated with celebrities to encourage those who had visited the hotspots on that day to identify themselves to the police.

Existing barriers to the adoption of TraceTogether

Ms Teo Yi-Ling, Senior Fellow, Centre of Excellence for National Security, S. Rajaratnam School of International Studies, spoke about the use of TraceTogether. The app, which was launched by the government in March this year, has had a low level of reception among citizens. Ms Teo presented three possible reasons for the low adoption rate of TraceTogether.

The first reason is people's fears over the loss of privacy. Such fears arise largely because of existing gaps in their knowledge pertaining to the types of personal data that can be gathered and used by the government. In addition, the absence of constitutional right of privacy in Singapore has created an uncertain and amorphous nature for privacy rights and laws in the minds of people. Consequently, this deters them from wanting to engage in further discussions or attempts to learn more about the use of the app altogether. In response to Dr Soon's question on why people are still uncomfortable with digital surveillance in Singapore given the omnipresence of closed-circuit television (CCTV) installed in various places, Ms Teo explained that CCTVs are usually placed far away from the sight of people, thereby making them oblivious to such surveillance. However, this is not the case with digital surveillance apps like TraceTogether which operate on smartphones and create a heightened awareness of being closely monitored.

The second reason relates to people’s concerns over possible cyber and data attacks. In recent years, Singapore has experienced various cyber attacks targeted specifically at the government’s database. One example is the SingHealth data attack in 2018. Hence, there is a fear of such cyber attacks recurring, which may compromise people’s personal information.

Third, there are problems associated with the functionality of TraceTogether. Currently, the app functions according to Bluetooth signals generated by smartphones. However, the reliance on Bluetooth signals tends to easily drain the battery life of smartphones, which deters people from wanting to use the app. She also acknowledged that during the circuit breaker period, the app was perceived as redundant as many people were staying in their homes. However, with the gradual re-opening of the economy in the upcoming weeks, TraceTogether would become increasingly more important.

Ms Teo added that the apparent ambiguity in government messaging regarding the downloading of TraceTogether has caused confusion among some people. In the past, the government has been direct in enforcing certain regulations on its citizens in the interest of public welfare. However, in the case of TraceTogether, despite being a strong advocate of the app, it has refrained from making its subscription mandatory for people. The ambiguity in government messaging could be due to what appears to be a modification in the social contract negotiation between the state and its citizens over the use of the app.

She briefly mentioned the existing psychological factors that discourage people from subscribing to the app. For example, some people are resistant to the idea of hearing bad news and therefore, prefer to be kept in the dark. Others are reluctant to use the app as it requires them to engage in a two-way communication with the authorities, unlike other apps like OneService where people do not have to engage in any follow-up. The prevalence of optimism bias — where people tend to assume that they are less likely to contract the virus as compared to others — also causes them to view the app as unnecessary. Ms Teo concluded her remarks by emphasising why TraceTogether was developed in the first place. She stressed that the app was created with the intention of supplementing manual contact tracing efforts. While it is an important development, it should not be regarded as the ultimate “silver bullet” in combatting the spread of the virus.

Sharing of personal data a civic responsibility?

Next, Mr Christopher Gee, Senior Research Fellow, Head of Governance and Economy, IPS, shared two possible trajectories that people could choose regarding the sharing of their personal data.

The first, which has been the current response of many, is to have an excessively cautious and fearful attitude towards the sharing of their data. He reasoned that this is usually born out of concerns over the possible misuse of their data by the government. Mr Gee cautioned that such a response can cause the complete withdrawal from online and digital spaces by everyone. This will lead to an expensive data security arms race, the cost of which will be shouldered by every citizen. The second, which he advocated for in today's data-driven societies, is to accept the principle that some private data must be considered as a public good, much like highways and nature reserves. He stressed that aggregating aspects of private and public data can help smart cities to better plan infrastructure, overcome negative externalities and improve amenities at both the micro and macro levels. Some existing examples of how such sharing of private data has benefitted individuals and the larger society include traffic congestion monitoring apps like Waze and electronic health records that have been anonymised and aggregated.

Mr Gee expressed confidence that people in Singapore would embrace digital surveillance apps like TraceTogether and Safe Entry. This is because they understand that the country's high level of socio-economic success generates various forms of negative externalities such as traffic congestion, environmental degradation and wider spread of diseases. Therefore, they have been cooperative, albeit reluctantly, in surrendering some of their personal rights to overcome some of these externalities. An example of this is the adherence to the mandatory wearing of face masks in public. Similarly, it is likely that most people in Singapore will accept the mandated use of TraceTogether and Safe Entry once the technical issues associated with them are resolved. Mr Gee concluded his remarks by emphasising that the sharing of private data should be regarded as a civic responsibility for all members of the society to adhere to.

Discussion

Measures to address privacy concerns

During the discussion, Dr Soon referred to a question posted by a forum participant on measures that the government could adopt to mitigate citizens' concerns and fears over the misuse of their data by the government. She also asked the speakers how they thought the government could further improve its public communication to help people better understand how their data was being collected and used.

Ms Teo said that it is important for the government to work on building greater trust with citizens. This can be achieved by ensuring that government communication remains clear, consistent and concise. It must also remain inclusive and be transparent in providing information on the security measures taken to protect people's data. She explained that people are generally comfortable with sharing their data with private corporations, rather than with the government. This is because, unlike private corporations, the government is not explicit in informing people what they get in return when sharing their data. Therefore, it is important for the government to broaden conversations with people on the collection and use of their personal data. However, this is not an easy task as it depends largely on the prevailing circumstances, which can limit the extent of information shared with the people. Dr Soon added that apart from the government, private developers of such apps must also design explicit guidelines and best-practice recommendations on how data will be used and secured.

Presenting a slightly different view, Mr Gee shared that instead of relying on the government to dictate the terms on the sharing of data, citizens should step up to take control over their attitudes and relationship towards their personal data. This can be done by people coming together to collectively establish a Digital Citizens’ Charter, similar to those in Canada and New Zealand. He said that in the context of Singapore, the charter can be more personalised and self-organised, and it should clearly outline the principles which individuals agree to on the use of their personal data.

Associate Professor Sonn agreed with Ms Teo and Mr Gee that it is necessary to consider the specific conditions under which the government can use citizens’ personal data. He suggested designing a positive list that clearly states the different types of data that the government can have access to in different situations. Currently, the Korea Centre for Disease Control and Prevention (KCDC) has been able to access citizens’ mobile phone and credit card data because of a revised law for the prevention and control of infectious diseases. The law was passed in the aftermath of the Middle East Respiratory Syndrome (MERS) virus in 2015. In addition to this, the police must also provide its approval for the KCDC to access individual’s data. Therefore, the government has been largely transparent in the collection and use of citizens’ data. However, this law has been problematic to some extent as not everyone is comfortable with having their identities revealed, such as members of the LGBTQ community. To overcome this problem, he proposed having a negative list alongside a positive list that clearly states what the government is not allowed to do with the data collected.

In response to a question on South Koreans’ cooperation in letting the government collect and use their personal data, Associate Professor Sonn explained that the country’s previous experience with the MERS outbreak provided valuable lessons for the government. During the outbreak, the government then had decided to restrict the sharing of information with the public. Hospitals that were treating confirmed patients were not allowed to provide information on how they were managing the situation. However, the government was forced to change its stance when a hospital was discovered to have become a hotspot for the virus to spread. To prevent the repeat of such an incident, the current government has maintained a transparent approach towards the sharing of information with its citizens right from the beginning. This has allowed it to gain the trust and confidence of its citizens who in return cooperate with the government’s contact tracing measures.

How should we view data?

Moving onto the topic of data-sharing beyond the pandemic, Mr Gee talked about the different situations in which data-sharing can provide mutual benefits for people. In the sharing economy, people are matched with others in the online space. Examples of these include delivery apps, ridesharing apps like GrabHitch and volunteering platforms that match people to suitable beneficiaries. Other applications of data-sharing include secure signing of contracts, receipts of digital documentation and responding to calls for help by the disabled and the elderly population. Ms Teo agreed with him that it is time for people to begin viewing data differently. Data today has become a highly valuable and inexhaustible resource, which has been exploited by the market in various ways. Hence, people need to recognise and understand the need to have greater control and, more importantly, provide informed consent over the collection and use of their data by both the government and private corporations.

Dr Soon asked whether there is a possibility that the Singapore government will make the use of TraceTogether mandatory in the future. Ms Teo said that this is highly unlikely unless the virus outbreak worsens. Mr Gee expressed a different view where he shared that the present situation has created a stronger need for the government to make TraceTogether mandatory. He reiterated his earlier statement where, like the case of face masks, most Singaporeans will learn to accept TraceTogether eventually. However, he expressed concerns over the implication of this on the long-term relationship between the people and the government. The mandated use of TraceTogether may affect the way in which people might react when the government approaches them to provide more data in the future.

Concluding remarks

In the final segment of the forum, the panel discussed on two key problems associated with the sharing of personal data. The first problem is the possible exclusion of certain vulnerable populations such as the elderly, people with disability and those without access to technological devices. The second problem is potential harms such as cyberbullying and doxxing of individuals. Associate Professor Sonn said the exclusion of vulnerable populations is less of a concern in South Korea. This is because even with a basic 2G mobile phone, the government will still be able to gather the location data of people. While he acknowledged that there is a small group of people who do not have phones, he said that they are less likely to be exposed to the virus and there are other tracing means such as the use of transportation cards available. In the case of cyberbullying, he recognised that it is a serious problem that can occur even when the exact details of the patients are not revealed. He suggested that to mitigate this problem, the government can consider publishing locations of potential infections in a general way, without linking them to specific case numbers of patients.

Mr Gee mentioned the Singapore government’s Digital Readiness Inclusion Blueprint, part of which focuses on digital inclusion in Singapore. The current pandemic has shown a strong reason for the government to accelerate this blueprint so that the country’s digital space will be made accessible to as many people as possible. Echoing his sentiments, Ms Teo shared how this pandemic has revealed the problems that exist within individuals and the society as a whole. The pandemic provides a *tabula rasa* moment in allowing us to reflect on many longstanding issues and rethink of new ways to overcome them and move forward.

Nandhini Bala Krishnan is a Research Assistant at IPS.

*****

If you have comments or feedback, please email ips.update@nus.edu.sg