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

RSIS COMMENTARY

www.rsis.edu.sg No. 040 – 17 March 2020

RSIS Commentary is a platform to provide timely and, where appropriate, policy-relevant commentary and analysis of topical and contemporary issues. The authors' views are their own and do not represent the official position of the S. Rajaratnam School of International Studies, NTU. These commentaries may be reproduced with prior permission from RSIS and due recognition to the author(s) and RSIS. Please email to Mr Yang Razali Kassim, Editor RSIS Commentary at RSISPublications@ntu.edu.sg.

Personal Data: Its Value, Risks & Potential

By Teo Yi-Ling

SYNOPSIS

Singapore, with its trusted data and analytics hub ambitions, may have lessons to learn from the slew of recent moves by the US. Federal agencies made some of the country's largest telecommunications and technology companies accountable for mismanagement of US citizens' personal data.

COMMENTARY

ON 28 FEBRUARY 2020, the United States Federal Communications Commission (FCC), the regulatory agency overseeing communications by television, satellite, radio, wire, and cable across the US, announced that it was going to propose some of its most substantial financial penalties against four of the largest US mobile networks carriers.

These proposed penalties, in excess of US$200 million, would be in respect of these carriers – Sprint, T-Mobile, AT & T, and Verizon – selling customers' real-time location data. This would be the first instance of the FCC addressing this issue of location data transactions in terms of privacy invasion.

Free Market Failures

For some time now, there has been a thriving market in location data and the lack of regulation around it, as highlighted in an earlier commentary addressing the issue of data privacy erosion and security.

Countries that have the business presence of some of these carriers, as well as countries that have data hub ambitions – like Singapore – will be watching this move

by the FCC very carefully, as the outcomes of this will have accompanying ramifications for compliance and governance.

While carriers have been allowed under US federal law to use location data for providing services like medical emergency alerts, fraud prevention, roadside assistance, and monitoring human trafficking, a report last year disclosed that some carriers were selling data to private individuals like car salesmen, property managers, bail bondsmen and bounty hunters, even after undertaking publicly to curtail this activity.

The contracts that the carriers had entered into with their customers (who commonly 'consent' to the wide 'standard terms' of the contracts because they have no choice) had not been effective at preventing such unauthorised behaviour, as the carriers had reneged on their own contractual obligations. This essentially meant that millions of smartphones were being tracked for apparently illegal purposes.

The scale of the issue is considerable – data of hundreds of millions of individuals owning smartphones were being continuously aggregated and traded. If triangulated correctly (for example with purchasing data or locations visited), such data does reveal personal and intimate details. Further, it may be the case that such aggregated data is feeding the already-thriving black market for data operated by cyber criminals.

Market Corrections

Such data selling-on is widespread among app makers and other technology companies (e.g. Facebook, Google and Tik Tok), but the telecommunications sector is subject to more stringent laws concerning the protection of customers' privacy, given that carriers have more access to their customers' personal data.

Given the existing regulatory framework, the fact that that a small group of the largest telecommunications players collectively failed in their legal obligations, makes the situation more egregious and concerning. Observers have noted that even if the fines are imposed, the quantum is manifestly inadequate, and would not meaningfully serve as a deterrent.

Notwithstanding issues of quantum, addressing deficiencies on the part of the telecommunications players is the next logical step, following from regulatory tightening taking place further upstream on the supply chain, nearer the sources of data, in order to properly manage accountability.

In the last 12 months, the United States Federal Trade Commission (FTC) has taken action in this respect against putative data collectors.: the $5 billion fine imposed on Facebook over the Cambridge Analytical scandal, the fine of $17 million on Google for violating the privacy of children on YouTube, and the fine of $5.7 million on the social media app Tik Tok over collecting data on underage children.

Data as a Regulated Resource

Could such enforcement be the impetus of rationalising data as a scarce resource? As has always been the case, useful resources are eventually subjected to regulatory

action to prevent monopolistic or dominant market power abuse, impose transparency, and provide protection for consumers.

Could a push for more comprehensive regulation then have a knock-on effect of crystallising the notion of personal data as property, capable of being owned and controlled?

Once given away, the value of data increases exponentially in the hands of those entities whose business models are predicated upon the collection and exploitation of data. To cast this situation in the cold light of day, this is an extremely one-sided and exploitative trade practice: large entities acquiring tangible value over the trade and monetising of volumes of data obtained all too easily.

The original source of the data – the individual – is left standing in a position that is worse off, having little or no control of how the data is used against him or her. Leaving the issue to market mechanics has so far proved ineffective in terms of protecting the value of data.

Policymakers need to consider whether real value must be given in return to the individuals, upon whose personal information and the transactions thereon, a gargantuan and insatiable demand for data has arisen.

Looking Ahead, Staying Grounded

The future posits shifting to more digital paradigms than less. Personal data utility will continue to be reshaped, redefined, and refocused, with the market naturally taking the lead. Singapore's transition to a Smart Nation and its data hub ambitions are about sustainability and survival through capitalising data, with the challenges of calibrating this against protecting the interests of its people.

All policymakers whose work touches personal data, not just the Data Protection Officer or even Personal Data Protection Commission, must continue to be closely attuned to the ramifications of this current paradigm of digital data exploitation, as digitalisation reveals aspects of peoples' lives that were once not so easily observed in an analogue world.

Personal data finding its way into the wrong hands is dangerous, and personal data taken out of context can be weaponised against individuals and those closest to them. The value of personal data is at once tangible and intangible - beyond notions of economic utility, the matter of data privacy strikes further and deeper: while personal data manifests our identities, more fundamentally it is about the natural right to be left alone.

This is the ability to decide the parameters of acceptable intrusions of informational, physical, and communicational privacy, which is priceless. Ultimately, it stands to reason that if the ability to control and deal in personal data is taken away from an individual, the ability for personal self-determination and free will – the power to decide one's thoughts and actions – is also then threatened.

Teo Yi-Ling is a Senior Fellow with the Centre of Excellence for National Security (CENS) at the S. Rajaratnam School of International Studies (RSIS), Nanyang Technological University (NTU), Singapore. She is part of the Cyber and Homeland Defence Programme of CENS.

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