The Right of Privacy : Death By a Thousand Data Cuts?

Teo, Yi-Ling

2019

Teo, Y.-L. (2019). The Right of Privacy : Death By a Thousand Data Cuts? (RSIS Commentaries, No. 052). RSIS Commentaries. Singapore: Nanyang Technological University.

https://hdl.handle.net/10356/80661

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

RSIS COMMENTARY

www.rsis.edu.sg No. 052 – 22 March 2019

The Right of Privacy: Death By a Thousand Data Cuts?

By Teo Yi-Ling

SYNOPSIS

Singapore has the goal of creating a digital data-driven ecosystem that will enable its "Smart Nation" vision, which promises to positively transform the way its citizens and residents live and do business. What does this mean in terms of citizens' privacy rights?

COMMENTARY

SINGAPORE'S APPROACH to data privacy protection is not the human rights-centric approach favoured by the European Union. It is also not the threat-based technology response that has driven reform in the United States. It is largely motivated by the forces of globalisation. And the necessity of adopting standards that will instil trust in its state entities, and allow for seamless integration into global networks.

In line with its Smart Nation vision, Singapore is being positioned as a trusted international data and analytics hub. It is where data flows in and out of the country will be enabled. Singapore's participation in the Asia-Pacific Economic Cooperation (APEC) Cross-Border Privacy Rules (CBPR) and the APEC Privacy Recognition for Processors (PRP) was approved in February 2018. The APEC CBPR System requires participating businesses to implement data privacy policies consistent with the APEC Privacy Framework (Framework).

The Right to be Left Alone

Essentially, the Framework seeks to provide for the protection of personal data by CBPR members. This is done while facilitating regional information transfers to benefit individual consumers, businesses, and governments.

It is also necessary to remember that alongside its obligations under the Framework, Singapore is a member state of the ASEAN Human Rights Declaration, which provides at Art 21:

"Every person has the right to be free from arbitrary interference with his or her privacy, family, home or correspondence including personal data, or to attacks upon that person's honour or reputation. Every person has the right to protection of the law against such interference or attacks."

This right to privacy – also defined as the right to be left alone – was enshrined to protect people from interference by state authorities and private persons, except by sanction of law. Classically, two concepts of privacy are mental (or communicational) privacy and informational privacy.

The former is explained as the ability to be alone with one's thoughts, wishes and feelings, to record these in written or electronic form, and to communicate the same to persons of one's choosing, without being eavesdropped upon or suffering other sorts of psychological intrusion.

The latter is described as protection for personal information which is legitimately (according to law and with the owner's consent and knowledge) held by public and private entities. This is on condition that disclosure of this information to third parties is prohibited.

Profiteering from Interference

With so much of modern life being driven by personal data, it is difficult to say that people are "free from arbitrary interference" as regards their privacy. Now the entities that appear to be interfering with these types of privacy are not so much state authorities, but businesses and their marketing efforts.

Enabled by algorithm-driven apps and the major social media platforms, they track every move and decision people make online (via their PCs and mobile devices) and predict behaviours. Location tracking is just one example of such interference. This industry had its roots in creating app customisation for smartphone users by providing advertising for nearby businesses.

A smartphone contains its user's contacts, call logs, memos, text and instant messages, images, videos, and GPS data. As smartphone and other mobile device use is commonplace and tracking technology is becoming increasingly accurate, this industry has grown capabilities in data collection and analysis, based on surveilling people's day-to-day activities.

The outcome of this is increasing intrusiveness. This is where high volumes of targeted unsolicited advertising are being received by people via their smartphones, or on social media.

It is not as though people are ignorant of the fact that apps are tracking their

movements: location companies make no secret that when location services are enabled by smartphone users, their data is easily collected.

Smoke and Mirrors?

Notwithstanding this, the explanations provided by apps about use of data – when users are prompted about granting location access – are often imprecise, oversimplified, or misleading.

An app may inform users that providing access to their location will then allow them to receive some specific information. But it may not explicitly disclose that collected data will be shared with or sold to third parties: advertisers, retail businesses; even financial institutions and hedge funds that invest in technology start-ups.

That disclosure is often found in a broadly-phrased, often non-negotiable privacy policy that is not immediately accessible to users, or may require clumsy toggling between online interfaces for access.

Even if these businesses maintain that they are only keen on understanding patterns of behaviour that the data may reveal, and not user identities per se, there is something egregious about this:

They keep users in the dark about how their data is exploited, denying them the ability to give informed consent or otherwise to such exploitation, and then use this data to intrude upon them digitally with volumes of unsolicited advertising, in the name of "personalisation" of information.

Preventing the Digital Erosion of Privacy

So it is not just the spectre of data breaches that the APEC states should be concerned about as threats to their citizens' privacy. It is also this seemingly cavalier attitude taken by businesses in what effectively amounts to wholesale dealing in personal data. Surely there has to be increased enforcement against such activity, or even the creation of more focused legislation as well.

With the progress of time and technology, it appears that privacy is being swiftly eroded. It is sobering to think that with digitisation, the notion of privacy (and its related right) may inadvertently cease to be a viable one.

It remains to be seen how Singapore and other APEC member reckon with the challenge of balancing their digital business ecosystem goals, with domestic laws and treaty obligations concerning privacy and data protection.

If cyber security protections for the personal data economy are not meaningfully enforced, consumer trust in engaging with online services, whether provided by the private or public sector, will suffer.

Teo Yi-Ling is a Senior Fellow with the Cyber and Homeland Defence Programme of the Centre of Excellence for National Security (CENS) at the 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