Source: *The Straits Times,* pA28
Date: 2 September 2017

ByInvitation

Privacy and our digital selves

Five years after Singapore first adopted laws on personal data protection, the pace of the digital revolution shows no sign of slowing. Important amendments are now being considered, with the public asked to submit their views by Sept 21.

Simon Chesterman

For The Straits Times

By next month, the lamp posts in Orchard Road and in selected housing estates will be doing more than just illuminating the street. With cameras and other sensors installed, they will capture real-time information on traffic flow, the environment, pedestrian movement – and, potentially, security threats.

In his National Day Rally speech last month, Prime Minister Lee Hsien Loong mentioned this as an example of the Smart Nation initiatives being rolled out in the coming months and years.

Smart Nation is only part of a larger transformation in the way we interact with the world and each other digitally. Known loosely as the "fourth industrial revolution", its impact on the economy is already clear: The world's biggest taxi service (Uber) owns no vehicles and the largest hotelier (Airbnb) owns no property; the most comprehensive retailer (Alibaba) holds no inventory and the most valuable media company (Facebook) creates virtually no content.

The vital commodity in this new digital economy is data, especially personal data. That economic reality is clear, yet our politics and laws remain fixed in 20th-century ideas of countries exercising jurisdiction over their fenced-off portions of the planet, while individual consumers contract with organisations that wish to collect, use and disclose their data.

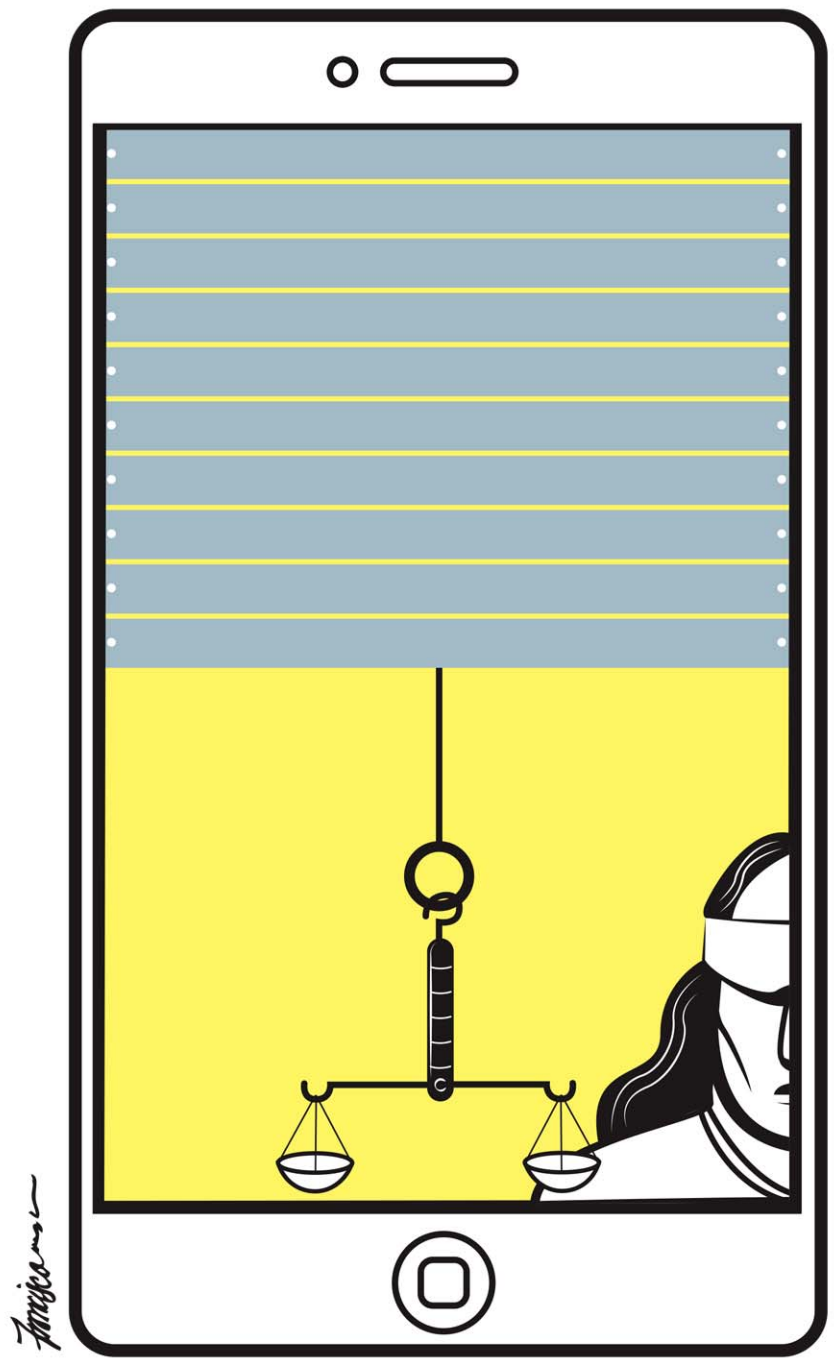
The Prime Minister's statement was timely because the Personal Data Protection Act (PDPA) is undergoing its first significant review since its adoption in 2012. A consultation paper seeks public comment on two key aspects of the legislation: whether organisations should be able to collect, use or disclose personal data without the consent of individuals, and what companies should do when the personal data they hold is lost or stolen.

BY CLICKING ON THIS LINK, YOU CONSENT

The foundation of most data protection laws is consent. In theory, when your personal data is collected, used and disclosed, that is in accordance with your agreement – often through a contractual arrangement with an organisation. In practice, of course, you just click "I accept" and get on with what you wanted to do.

In any case, you would be wasting your time if you read the multi-page end-user licence agreements. Not even law professors bother to do so. The British retailer GameStation gave us memorable proof of this one April Fool's Day, when more than 7,000 people clicked "I accept" to terms and conditions that included the surrender of their immortal souls to the company. (The company later rescinded all claims, temporal and spiritual.)

As computing becomes ubiquitous, the sheer volume of data being collected will make this artificial notion of consent start to seem ridiculous. Do we really need to "agree" with our phones, the lamp posts, Wi-Fi routers, bus route optimisers, autonomous vehicles and so on, so that they can collect and use basic personal data?



Even if we did, the sheer volume of such "agreements" would lead to consent fatigue, making it hard for us to distinguish harmless services from selling our immortal soul – or, worse, exposing ourselves to identity theft. There are also circumstances where consent might not be desirable. If data is collected to guard against a security threat or detect fraud, requiring individual agreement may frustrate that purpose.

The 2012 law does allow for consent to be "deemed" in limited circumstances, or circumvented when necessary in the interests of the individual or for an investigation or certain forms of research. But this may not cover data collection that is intended to benefit a larger population, for example through analysis of customer profiles that include personal data.

In some circumstances, it may be appropriate to rely instead on a regime of notification and accountability. Organisations would be obliged to notify individuals – such as through an appropriate sign – and be accountable for collecting, using and disclosing personal data only in a manner that will have no adverse impact on the individuals concerned.

Mr Warren Buffett famously said that it takes 20 years to build a reputation and five minutes to ruin it. In today's digital economy, a reputation can be built much faster than that – Uber, Airbnb, Alibaba and Facebook are all under 20 – but you can lose that reputation in a nanosecond.

That accountability should not only be invoked after something goes wrong. One possibility is that organisations be required to conduct a data protection impact assessment, putting in place measures to mitigate the risks that come with such an approach.

ONCE MORE UNTO THE BREACH

But what happens when something does go wrong? Given the volume of personal data being collected, breaches are already depressingly common.

We may have sniggered when Ashley Madison, the extramarital affair broker, had its records leaked – revealing that 31 million men were, for the most part, chatting with bots and not actual women. But Yahoo recently disclosed that 1.5 billion accounts had been hacked, while in South Korea nearly half the population had their credit card details stolen. The potential for a data breach to affect any one of us should be clear.

As Singapore's 2012 law was being drafted, there were suggestions that it should include a requirement that organisations notify users when a data breach occurs. This did not make the final Bill due in part to concerns that it could be unduly onerous. Sensible companies notify their customers after a serious breach anyway – often mitigating the impact and in some cases the penalty – but practice has been inconsistent.

Trivial data breaches happen all the time: A requirement to notify every user of every breach would be akin to the proverbial boy who cried wolf. Key questions include what threshold should be established and within what timeframe organisations must inform users.

Australia recently passed legislation that will require organisations to notify affected individuals as soon as practicable if there are reasonable grounds to conclude that a breach is likely to result in serious harm to them. A new European Union regulation will similarly require notification of individuals without undue delay if the breach is likely to result in a high risk to their rights and freedoms.

Mr Warren Buffett famously said that it takes 20 years to build a reputation and five minutes to ruin it. In today's digital economy, a reputation can be built much faster than that – Uber, Airbnb, Alibaba and Facebook are all under 20 – but you can lose that reputation in a nanosecond.

Some companies are likely to complain about being compelled to issue bad news about themselves. But the reality is that the market punishes data breaches even more severely, particularly when they are covered up. Yahoo's data breach put a price on this, when Verizon slashed US$350 million (S$475 million) from its offer price for Yahoo's core Internet business after the hack was made public.

WATCHING THE WATCHERS

The elephant in the room, of course, is that none of this will apply to the Government and its lamp posts. The PDPA specifically excludes public agencies from coverage and allows that exclusion to be extended to any statutory body.

Government rules governing data protection are said to offer "similar levels of protection" – but as those rules are not themselves public, this claim is difficult to evaluate. With plans to roll out a new national digital identity scheme over the next three years, the need for trust in the Government's ability to safeguard the data of its citizens has never been greater.

Moves to ensure high levels of security in the public sector – including the extraordinary step of isolating hundreds of thousands of government computers from the Internet – show that these issues are taken seriously. Even as the private sector is being encouraged to hold itself more accountable to regulators and consumers, perhaps it is time for more transparency about the Government's own accountability structures in the handling of personal data.

I've previously written about the death of privacy (spoiler alert: we killed it ourselves). It is telling that the PDPA and the new EU regulation barely mention that word. Such data protection laws are best thought of not as protecting an individual's intimate thoughts from the public gaze, but as managing the flow of information about us in an increasingly digital world.

As Smart Nation and the Internet of Things usher in a proliferation of sensors, and as we live increasing proportions of our lives online, it is time to rethink the fundamentals of data protection law. Otherwise we run the risk of using those principles the way a drunk uses a lamp post – for support, rather than illumination.

stopinion@sph.com.sg

• The writer is dean and professor of the National University of Singapore Faculty of Law and an unpaid member of the Data Protection Advisory Committee, which advises the Personal Data Protection Commission on review and administration of the personal data protection framework.