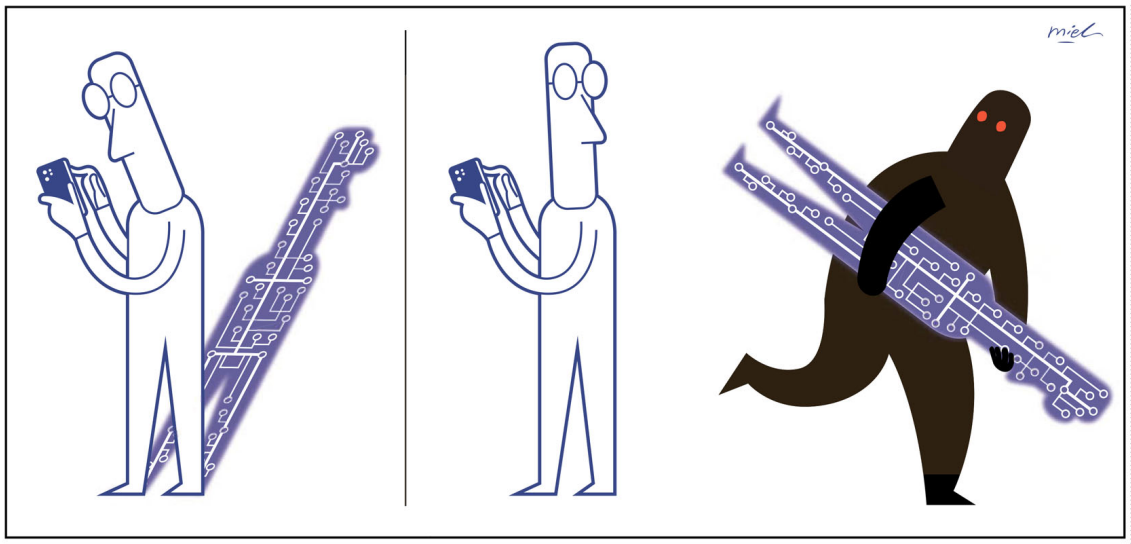
Source: *The Straits Times*, pA20
Date: 17 October 2020



By Invitation

Your data or your life

Singapore's data protection regime is eight years old. It's time to grow up.

Simon Chesterman

For The Straits Times

Data, in particular personal data, is often described as the "new oil" powering the information economy. It's an attractive metaphor – evoking transformations under way in a fourth industrial revolution, heralding a world of artificial intelligence and limitless possibilities.

Unfortunately, that metaphor is wrong in almost every way.

Oil is finite, companies pay millions to extract it, and each barrel can be used only once. Data, by contrast, is infinite, consumers give it to you for free, and you can keep using it for as long as you like.

Eight years ago, Singapore adopted the Personal Data Protection Act (PDPA) – not long after the release of the iPhone 5, back when Snapchat was a hot new app.

Subsequent years have seen a massive expansion in the data-driven economy, with the full benefits yet to be realised.

The digital transformation has been overwhelmingly positive. We connect with others and access resources more easily than at any time in human history. This was a boon during the pandemic. As difficult as lockdowns have been in Singapore and around the world, imagine working from home if you had only a 2G phone and a dial-up Internet connection.

The darker side, of course, is that "surveillance capitalism" is funded by exploiting our data. Data is not the product being bought and sold: we are.

Breaches such as that experienced by SingHealth in 2018 are useful reminders that another downside of convenience is risk. That same year, Cambridge Analytica showed that personal data could be used to steal elections as well as identities.

And so earlier this month, the Government introduced the first major amendments to the PDPA. As Parliament prepares to debate the new law, here are three questions worth keeping in mind – plus a bit of extra homework.

1 I SHARE, THEREFORE I AM

First, what is data, anyway?

We routinely talk about "our" personal data and get upset when someone "steals" it. Is our data a piece of property, like a bicycle?

When Facebook chief executive Mark Zuckerberg testified before the United States Congress in 2018, he repeatedly said "people own all of their own content". Maybe our personal data is closer to copyright?

The problem with thinking of personal data in either of these ways is that they fail to recognise its true value and the ongoing interests of the individual identified by it – even if he or she chooses to "sell" it.

You cannot, in any meaningful sense, "sell" your personal data. Moreover, society has an interest in treating personal data as more than a commodity that can be bought and sold.

Your name, for example, is not used merely as a personal identifier or as a social marker for the convenience of friends and family. It also has legal significance: We are assigned it at birth, use it to pay taxes and vote, enter it into a register when opening a bank account, and so on. In Singapore the National Registration Identity Card plays a similar role.

This question is of more than academic interest, because it highlights a fundamental flaw in the personal data protection regime to date.

The PDPA, like most such laws around the world, relies heavily on consent.

In theory, when your personal data is collected, used or disclosed, it is on the basis of an agreement between you and the organisation doing so. Typically, this takes the form of a contract with hundreds or even thousands of words.

In reality, of course, you don't read the terms and just click on "I accept". (I'm a law professor who has published books on data protection, and even I don't read them.)

As computing becomes ubiquitous, the idea that we transfer property or some other kind of right dozens of times a day with each "agreement" won't just be an academic problem but a practical one as well.

Rather than relying on artificial notions of consent, the amendments recognise that organisations may have a legitimate interest in collecting personal data.

Instead of putting the onus on the consumer to read the fine print in all cases, the obligation will fall on the organisation to provide proper notification and guard against any "adverse effects".

2 ONCE MORE UNTO THE BREACH

This leads to the second question. When organisations are collecting ever more personal data, how can we best protect it?

One way is by letting the punishment fit the crime.

In 2012, the $1 million fine in the PDPA sounded like a lot of money. Then in 2018, the European Union's General Data Protection Regulation (GDPR) introduced a fine of €20 million (S$32 million) or 4 per cent of annual global turnover – whichever is greater. For Facebook, that could mean a fine of $4 billion.

Not to be outdone, the PDPA amendments initially proposed fines of up to 10 per cent of annual turnover.

As Sean Connery's character quipped in The Untouchables: Don't bring a knife to a gunfight.

Based on feedback during the public consultation period, however, this is now based on turnover in Singapore.

Fines usually come too late to help consumers, anyway. More important are new requirements to undertake risk assessments and mandatory data breach notifications.

The sooner consumers know about their data being lost, the sooner they can protect themselves. Even if there is no "harm", requiring organisations to report on breaches improves accountability and transparency – ultimately increasing trust.

But where to set the threshold? Too low and every time an e-mail is misdirected a notification must be submitted – the Personal Data Protection Commission will be buried in reports. Too high and breaches that foreshadow systemic risks may be missed.

The amendments propose that breaches must be reported if they are "likely" to cause "significant harm" or affect a significant number of individuals – likely set at 500. "Significant harm" appears broader than the GDPR threshold of "high risk" to a person's rights and may need to be clarified in practice.

In most circumstances, the organisation must notify affected individuals "as soon as practicable" and advise the commission within three days.

Another welcome increase in accountability is that individuals will be held personally responsible if they knowingly or recklessly use or disclose personal data without authorisation – with penalties of up to a $5,000 fine or two years' imprisonment.

This mirrors the penalties for public officers introduced two years ago in the Public Sector (Governance) Act, which is broadly aligned with the PDPA. (Singapore is unusual in that the PDPA exempts public agencies from coverage, though the Government has long argued that internal manuals and legislation such as the Official Secrets Act provide adequate protection.)

3 DRIVEN BY DATA

While the GDPR's explicit purpose is to protect human rights, Singapore's PDPA was always a pragmatic compromise between the rights of individuals and developing the digital economy. That raises the third question: What does all this mean for business?

The net impact of the changes should make it clearer to organisations when they can use data.

Rather than adding fine print to contracts that no one reads, they can use data analytics for business improvement purposes, rely on a legitimate interest exception to guard against fraud or abuse, and use deemed consent to cover the multiple layers of commercial partnerships that underpin the purchase and delivery of goods online.

For consumers, it should mean more personalised services – with portability obligations increasing competition by lowering entry barriers and enabling users to move their data if they are unhappy or want to try something new.

4 DO NOT DISTURB

A final change might have been the most welcome: Closing the gap between the Spam Control Act and the Do Not Call Registry. Until now this left out some instant messaging services such as WeChat and Telegram.

It's a step in the right direction, but users will still need to go to the Personal Data Protection Commission for unsolicited marketing calls and texts, while scams and loan sharks must be reported to the police.

As for e-mail and other kinds of spam, enforcement is theoretically possible and penalties are increased – but you're better off investing in a decent filter and blocking irksome accounts.

Perhaps reconciling these problems could be the focus of future amendments.

There is a lesson here, however. Laws like data protection work best when they are seen least.

The purpose of data protection law is not to preserve privacy as such but to give users reasonable control over their data, reaping the benefits of the information economy while mitigating the risks and minimising the hassle.

So no, data isn't the new oil. Or if it is like oil, it's a lubricant rather than a fuel – not consumed to power the digital economy, but enabling it and accelerating it.

Be cautious, however. Because if you spread it around too liberally, you might just slip and fall on your face.

stopinion@sph.com.sg

• Simon Chesterman is dean of the National University of Singapore Faculty of Law. He is an unpaid member of the Data Protection Advisory Committee, which advises the Personal Data Protection Commission on matters relating to the review and administration of Singapore's personal data protection framework.