Source: *The Straits Times,* pA34
Date: 4 August 2018

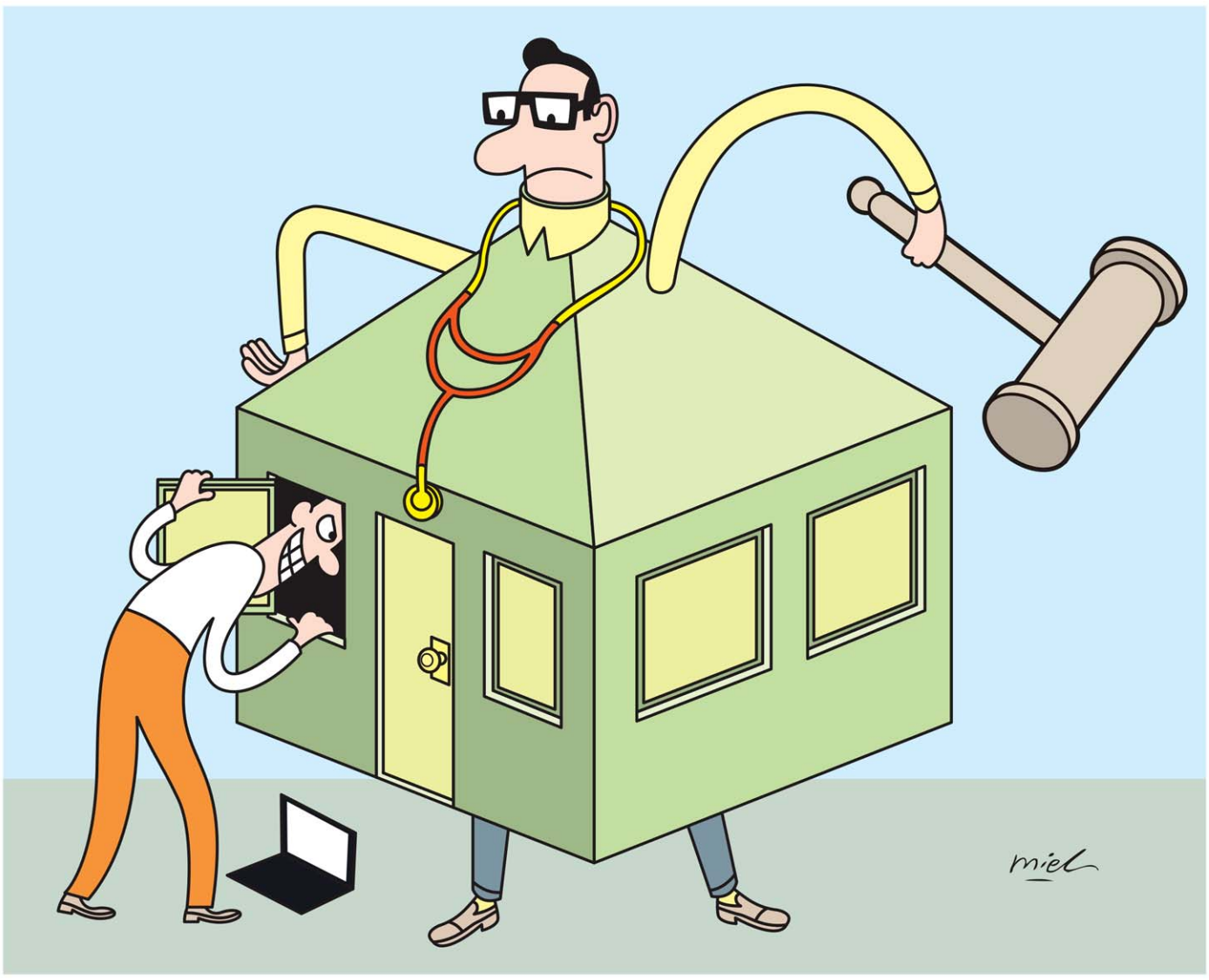
ByInvitation

SingHealth breach may give privacy new life

2018 is a bad year for privacy, but it can take a good turn if it sparks rethink of privacy issues

Simon Chesterman

For The Straits Times



Reports of the death of privacy are greatly exaggerated.

This might seem an odd opening line, with Singapore still reeling from its worst ever data breach, in which the personal details of 1.5 million people were stolen from SingHealth.

But as the country realigns its economy and its public institutions to take advantage of the digital revolution, 2018 could end up being the year in which cyber security is finally seen as everyone's problem – and in which privacy is one of the things we aim to secure.

For two decades, boosters of technology and jaded academics (myself included) have quoted the former chief executive officer of Sun Microsystems, Mr Scott McNealy, who infamously declared in 1999 that privacy was dead and everyone should just "get over it".

That was back when Mr Mark Zuckerberg was still in high school and before Apple had even launched its first iPod. The subsequent years seemed to bear Mr McNealy out: Governments spied on their people, corporations vacuumed up their data, and individuals seemed happy to share their innermost thoughts with the entire world on social media. Privacy was dead, buried and few seemed to mourn it.

Yet 2018 was the year in which privacy got a new lease of life. It was always going to be significant, as May 25 marked the long-awaited entry into force of Europe's General Data Protection Regulation (GDPR) – bringing with it huge fines of up to €20 million (S$31.7 million) or 4 per cent of a company's global turnover.

Two months earlier, however, the GDPR was upstaged by the Cambridge Analytica scandal at Facebook. Suddenly, rules like those in the GDPR that give users greater control over their personal data and the quaintly European "right to be forgotten" came to be seen as globally important. The changing market sentiment led Facebook to overhaul privacy settings, part of the reason for its historic drop in share price last week.

As for Singapore, last month's SingHealth data breach came at a crucial juncture in the Smart Nation initiative, forcing an overdue rethink on the tension between efficiency and security – and, perhaps, starting a conversation about privacy and trust.

SMARTER NATION

Two years ago, the Singapore Government's decision to isolate more than 100,000 computers used by public servants from the Internet was seen by many as an overreaction and even mocked. In the wake of the SingHealth breach, it could be argued that the Government did not go far enough.

The first point to note is that the recent breach could have been far worse.

The intruders could have stolen more sensitive data such as detailed medical or financial records, ransomware could have been installed, records could have been deleted or – worst of all – quietly amended. Change one patient's blood type, alter another's allergies, vary a third's medication, and so on.

The reasons for attacking SingHealth remain unclear, though Prime Minister Lee Hsien Loong's medical records were specifically targeted. It has been reported that evidence points towards a state actor, which might be good news for those whose data were stolen. A state actor is less likely to use the demographic information for identity theft than a criminal hacker. If true, the intent might have been more political than financial: demonstrating vulnerabilities in Singapore's systems and showing that they can be exploited.

Some of these questions may be answered by the Committee of Inquiry that will report its findings to the Government by December.

In the meantime, the SingHealth breach offers a useful opportunity to review how and why public and private databases in Singapore are linked up and what safeguards need to be put in place to protect them.

The most prominent step has been implementing a temporary Internet surfing separation policy in the healthcare sector, similar to that used in many government agencies here. This will introduce inefficiencies, with doctors and staff toggling between devices if they need access to the Internet – but unless alternative measures can be found to guard against cyber attacks, it could well become permanent.

Those alternative measures – such as encryption protocols, firewalls, and industry best practices such as the ISO 27000 family of standards – are only partly technical. As banks and other actors safeguarding sensitive information know, and as hackers these days exploit, the weakest link in any security system is the venality and gullibility of its human users.

Surely, one might argue, it should be possible to train Singapore's well-qualified and well-paid officials not to respond to phishing e-mails or click on suspicious links? A partial answer is that even the social media accounts of Twitter CEO Jack Dorsey and Facebook's Mr Zuckerberg have been hacked in the past two years.

Hardening defences prioritises security over efficiency and will mean slowing down the Smart Nation drive, at least temporarily, though it is unlikely to stop.

VERIFY, BUT TRUST

This would be a missed opportunity, however, if the focus is solely on security. For the real damage in the SingHealth data breach is that it undermines trust.

Though SingHealth is a private entity and will, in due course, be investigated by the Personal Data Protection Commission (PDPC), the Government itself remains immune from the legislation governing how personal data is collected, used and disclosed.

The Public Sector (Governance) Act, passed in January this year, now imposes fines and jail terms for public sector officers who share data without authorisation. That is a step in the right direction, but taking full advantage of the digital age – and ensuring public confidence – would be helped by greater transparency about the full range of safeguards that exist, including how and why personal data are collected in the first place.

Of the 120 or so countries with data protection legislation, Singapore is in a very small group – together with Malaysia, Vietnam and India – where the relevant legislation excludes the public sector entirely.

When Singapore's law was first passed in 2012, then Minister for Communications and Information Yaacob Ibrahim stressed that the public sector has its own data protection rules, which are "guided broadly by the same principles". As those rules are not themselves public, however, the statement remains difficult to evaluate.

At the annual Personal Data Protection Seminar last week, Minister-in-charge of Cyber Security and Minister for Communications and Information S. Iswaran rightly stressed that responsible data protection is a "whole-of-Singapore endeavour, and we each play a part – whether it is the Government, private sector or the people sector – in ensuring robust practices to preserve trust in and among our institutions and organisations".

Moving forward, security and trust will both be important in taking full advantage of the opportunities presented by the digital age.

PRIVACY REBORN?

So does all this mean that academics (like me) writing about the death of privacy were peddling "#FakeNews"?

Possibly. Yet I think the main problem was that we were using the wrong metaphor.

Privacy is, obviously, not a living thing that can be killed. Privacy might be better thought of as a kind of public good, like clean air, national defence, or – as some economists now argue – health.

Much like privacy, we all claim to care about our health and yet we regularly do things that undermine it: We eat fatty foods and don't exercise enough, some of us drink and a declining number smoke.

We have the freedom to make such choices, but our freedom is not absolute because our choices affect other people. Governments around the world enact laws to ensure that food is of a certain standard. At the very least, it shouldn't poison you. And, increasingly, governments "nudge" their citizens to do things that are good for their health. Eat better; exercise more. Extra precautions are taken to protect children – compulsory vaccinations and so on.

It is possible that we could move in a similar direction with privacy. Instead of relying on contractual provisions that no one (even a law professor) reads, the public good associated with privacy could be safeguarded through laws that encourage good behaviour as well as punishing bad.

For example, data protection impact assessments are presently encouraged by the PDPC, but could be made mandatory for organisations and public agencies alike. Rather than relying on the nominal consent of users, the onus would be on the entity doing the collecting to justify why personal data is needed, how it will be used and to whom it will be disclosed.

Similarly, special protections for children have been in place in the United States for two decades and are included in the new GDPR, raising the legal requirements for collecting their data. In Singapore, this remains a guideline, though the legislation empowers the Government to change this through regulation.

"Never waste a crisis" is a line often wrongly credited to Winston Churchill. Whoever coined the phrase, it holds some wisdom. For SingHealth, for Facebook, and for privacy more generally, 2018 may be an *annus horribilis et mirabilis*: a year both horrible and wonderful.

Horrible for the breaches that occurred, yet miraculous if those breaches remind us of the value of what was stolen in the first place.

stopinion@sph.com.sg

• Simon Chesterman is dean and professor of the National University of Singapore Faculty of Law and editor of Data Protection Law In Singapore: Privacy And Sovereignty In An Interconnected World, published this week by the Singapore Academy of Law.