RSIS S. RAJARATNAM SCHOOL OF INTERNATIONAL STUDIES
Nanyang Technological University

RSIS COMMENTARY

www.rsis.edu.sg No. 036 – 17 February 2016

We, Citizens of Smart Singapore: Data Protection in Hyper-connected Age

By Tan Teck Boon

Synopsis

Data theft and abuse is expected to increase with hyper-connectivity. A more robust personal data protection regime goes hand in hand with a smart Singapore. What are the key features of this regime?

Commentary

AS SINGAPORE transforms into a smart nation, a more robust personal data protection regime is needed to safeguard the enormous amount of private information generated by this high-tech architecture. Underscoring the dangers of cyber intrusion and data theft, Hong Kong-based toymaker Vtech was recently hit by hackers who stole the personal data of five million customers worldwide.

Currently, the regime regulating personal data held by the private sector includes the *Personal Data Protection Act*, the *Telecommunications Act* and the *Banking Act*. In addition, the *Computer Misuse and Cybersecurity Act* oversees the unlawful access to data while the law of confidence criminalises unauthorised publication and misuse of private confidential information. The *Personal Data Protection Act* serves as a baseline legislation that governs general activities with the higher standards applying to specific areas (e.g., the *Banking Act* will apply for banking records).

Hyper-connectivity and its Discontents

While extensive, this personal data protection regime will no longer be adequate in the smart nation scenario. Although a more robust personal data protection regime will not wipe out data theft and abuse, it will at least make it more costly and difficult to do so.

In the smart nation, an array of Internet-enabled gadgets will generate a vast amount of personal data. However, the personal data generated by these gadgets will not only contain plain information like names, birth dates and contact details but also deeply private and revealing information like energy consumption patterns, geo-location data and even lifestyle habits. It is conceivable that citizens could be put at risk of serious financial and reputational losses if this information trove were stolen or lost and then used by criminals for illicit purposes.

To be fair, the smart nation is expected to engender a myriad of economic, societal and environmental benefits. The main issue though is that some of the Internet-enabled but resource-constrained gadgets endemic to this high-tech architecture might also open up more pathways for hackers to exploit. Given the revealing nature of the data in question, cyber criminals could in theory use these data for blackmails or scams.

As the number of Internet-enabled gadgets going online increases and the volume of revealing personal data swells concomitantly, the chilling prospect is that anyone with the slightest infraction – moral or otherwise – can become victims of cyber criminals.

Insider Theft

Apart from hackers exfiltrating personal data, employee theft will also be a matter of concern. If anything, insider theft of data are often more damaging than malicious attacks carried out by external hackers since the errant employee not only knows where the most prized data are stored but also how to gain access to it. And of course, personal data can be leaked into the open because of employee carelessness. While not particularly malicious, such breaches are nevertheless serious if the data lost were to fall into the wrong hands.

Because the data generated by the smart nation will also reveal a wealth of information on consumer preferences and tastes, businesses might also be tempted to data-mine this treasure trove for insights. From targeted advertising to ideas for the next product hit, the commercial reward can be tremendous. But the real danger is when the same insights are used to single out and penalise certain individuals. Consider what might happen to a man betrayed by his Internet-enabled gadgets to live an unhealthy and even risky lifestyle.

If that information were leaked to his health insurer, he will either be required to pay a higher premium or worse, denied health insurance altogether. And what if that information were uncovered by his employer? The question of whether he will be denied employment subsequently is a legitimate one.

While there is no evidence that such malfeasance has already happened despite the rapid proliferation of Internet-enabled gadgets in our homes, one should note too that it is now a common practice for tech companies to collect all sorts of user data ostensibly for troubleshooting purposes and to push advertisements. As companies get better at analysing and understanding the data they collect in the coming years,

the temptation to extract commercial rewards from this treasure trove will invariably be even stronger.

Data Protection in the Hyper-connected Age

What should a more robust personal data protection regime for the private sector in Singapore be like? At a minimum, the regime would need to delineate clearly which data sets belong to whom and more importantly, which data could be shared and aggregated. Apart from personally identifiable information (e.g., names, birth dates and contact details), data that can potentially reveal one's routine, lifestyle and movements should come under the regime's protection too.

Beyond that, it would need to place legal restrictions on the aggregation of personal information harvested from different Internet-enabled gadgets. This will at least make it more difficult for cyber criminals and errant businesses to piece together private information harvested from disparate sources and link specific data sets to individuals.

Encryption is one way to prevent personal data from being read when stolen or leaked but eventually, it might be worthwhile to consider ending the practice of having the private sector hold on to the personal data that it collects. With deeper domain expertise in cybersecurity and more rigorous practices in place for handling confidential data, the government might actually be in a stronger position to safe-keep personal data on behalf of the private sector.

If this were implemented, the risk of personal data theft will be significantly reduced and limited to when data are being transferred between points. The fact that major data breaches in Singapore have so far been confined to the private sector does lend some credence to this move.

Ultimately, a more robust personal data protection regime must go hand in hand with the smart nation. Indeed, when private citizens are convinced that their personal data are secure and well-protected, they will also be more likely to embrace and play an active part in this high-tech architecture. Hence, the issue of data protection needs to be addressed now and not when it is too late. That would be the smart thing for a smart nation to do.

Tan Teck Boon is a Research Fellow at the S. Rajaratnam School of International Studies (RSIS), Nanyang Technological University, Singapore.