OPINION

Protecting and sharing personal data

BY SIMON CHESTERMAN

BY INVITATION

B Y T H I S time Singapore's Do-Not-Call (DNC) Registry came into effect earlier this month, more than 400,000 numbers had already been entered online, by SMS, and by phone. Many Singaporeans, it is clear, are not particularly interested in unsolicited offers of investment advice, "exclusive" property offers, and so on.

But the reaction to the last-minute amendments to the DNC regime, in which a limited exemption was created for text messages, shows how hard it is to balance the theory and the practice of what is loosely called "privacy".

In theory, people do not want to be bothered by voice calls, SMS messages, and spam e-mail. The higher you raise that threshold, however, the more likely it is in practice that you will miss out on something you actually want or need.

In the case of spam, for example (which is not covered by the new law), it only takes a few seconds to delete unwanted messages. But it can take weeks to realise that an important e-mail was filtered out by overly-enthusiastic software.

Such was the thinking behind the DNC compromise—which, admittedly, came too late and should have been addressed at a far earlier stage of the public consultations.

By creating a limited exemption for text messages where there is an ongoing commercial relationship, it was hoped that companies and consumers would still be able to share relevant information while screening out the most annoying way of offering it.

It will be important that "ongoing relationship" is defined narrowly, and that any messages must relate to the subject of that ongoing relationship. This might include special offers from your credit card company or telecom service provider, but not follow-up solicitations after a single purchase or inquiry. The fact that you speak to an agent about one thing should not mean that he or she can then harass you about another.

The issue of how to balance the need to protect information against the importance of that information flowing properly will become even more complex when the rest of the Personal Data Protection Act comes into force in July.

The balancing act is complex because keeping information about oneself truly "private" is becoming both more difficult and less desirable.

It is more difficult because governments and corporations have access to more personal data about more people than at any other point in human history.

This goes well beyond the surveillance powers of the state. It includes the various "smart" devices that consumers routinely carry, siphoning up details of communications and movements.

As more daily interactions with the world take place online, it is far harder to know or analyse what data, developing profiles that track what consumers have done in the past and predict what they are likely to do in the future.

But keeping information truly private is also less desirable. This is because many conveniences of the modern world depend on interconnectivity. People depend on being able to communicate with anyone any time, purchase items quickly and easily, and have access to personal data anywhere on any chosen device.

The dangers of abuse and misuse of personal data are clear. Discount retailer Target, for example, recently revealed that over the holiday season, the credit card information of 40 million of its customers was stolen, along with the contact details of 70 million more.

That incident was a result of hacking, but incompetence can also cause damage. Only a few years ago, the British tax authorities lost two discs containing the names, national insurance numbers and banking details of 25 million Britons—almost half the population—when they were sent between offices as unsecured internal mail.

But if a data protection regime is too strict, it introduces transaction costs that cause delays and raise prices.

One way to illustrate this is to think of one's own approach to data protection. Most of us use passwords on a daily basis. To keep them secure, it would be prudent to use different passwords for every account, change those passwords regularly, and never use anything recognizable as a word or phrase. Most of us know this, but few people actually adopt such a regime because they conclude that it is not worth the bother.

In a globalised world, there is also a need to tailor data protection laws to international standards. One of the many interesting aspects of Singapore's Personal Data Protection Act is that it was driven not by the kind of human rights concerns that characterise Europe's approach to the topic, but by an explicit desire to balance the legitimate needs of business and the rights of individuals.

In his second reading speech, Minister for Communications and Information Yaacob Ibrahim emphasised that the purpose of the legislation was to "strengthen Singapore's overall competitiveness, and enhance our status as a trusted hub and choice location for global data management and processing services".

The marginal importance of privacy to all this can be seen in the fact that the word does not appear in the legislation at all.

In addition, public agencies are excluded entirely from its coverage. (When questioned on this in Parliament, the minister stressed that the public sector has its own data protection rules, which he said are "guided broadly by the same principles" as the PDPA. As those rules are not public, however, this statement is difficult to evaluate.)

The medium- and long-term impact of the legislation will, of course, depend on how it is implemented. There is evidence that the DNC Registry is already reducing the number of unwanted calls and text messages, and most businesses are preparing for the implementation of the personal data measures to follow.

In a post-privacy world, there are complex challenges. It is not surprising that a small industry has emerged to assist companies in complying with the new regulations, offering your services to help them out. My number is in the DNC Registry.