

THE STRAITS TIMES INTERACTIVE

STI Home > Review > Others > Story > Print

>> Back to the article

Aug 16, 2005

Protecting privacy of IC data

By Ivan Png

For The Straits Times

FOR every Singaporean, the identity card is a critical personal identifier. We need it for service at government offices and financial institutions, to apply for a bank account, credit card or mobile phone service, and even to gain admission to pubs. Yet the ways in which identity cards and IC numbers are used leave room for abuse and worse.

Open your daily newspapers. Frequently, you will see notices of lucky draw results with the full names and IC numbers of the winners. What purpose do such advertisements serve? They certainly are not legal contracts. The winner's basis of claim is his or her ticket. The ads need not publish full names and IC numbers to notify winners. Surely a name and partial IC number - like '1234XXX' - would suffice?

Enter any major commercial building, government office or even a private condominium. Following 9/11 and the Sars outbreak, visitors are typically required to declare their name, IC number and contact information.

Some institutions even require them to surrender their ICs for a visitor's pass. Who has access to those bulky record books filled with visitors' personal particulars? How are the records handled after the visitors have left? Who knows?

How often have you been asked to hand over your IC as a deposit for something so trivial as a toilet key?

In Singapore, we are lucky that identity theft is rare and credit card fraud is declining. However, this is no reason for complacency. In a United States Conference Board study, over 13 per cent of Internet users reported that they or a household member had experienced identity theft.

Fraudulent use of identity cards and IC numbers may be rare in Singapore, but it does occur. According to the Ministry of Home Affairs, in 2003-2004 there were nine reported cases involving the fraudulent use of another person's identity card. The perpetrators used another person's card to apply for mobile phone service or gain entry into pubs and bars.

Widespread Internet use has aggravated the potential for fraudulent use of IC numbers. In one case, the victim used his IC number as the log-in ID for a computer system. The system auto-saved the victim's log-in ID and displayed it on the log-in screen for the next user. That next user was the identity thief, who used a default company password to access the system.

It is time that we adopt best practices in the safeguarding of identity cards and IC numbers. Hong Kong requires all users of IC numbers to comply with a code of practice. The code disallows the public display of a person's name and IC number. Consequently, Hong Kong newspapers do not publish full names and IC numbers in announcements of lucky draws and share issues.

The Hong Kong code requires anyone who has recorded another person's name and IC number to limit access to the information.

Thus, a visitor to a building will not be allowed to peruse a book full of names, IC numbers and contact information of other visitors. The code also requires that the record be erased within a reasonable time.

Advertisers, for one, should take due care to protect the privacy of their clients and customers. There will, of course, be situations where exceptions are appropriate - for instance, notices of legal action and of bankruptcy.

In addition, it is time that property owners and managers in both the public and private sectors reconsider their record-keeping practices. They should ponder what personal information of visitors is necessary, collect it in a way that is not intrusive, and establish proper procedures for the safe-keeping of personal information and for the destruction of the records after a reasonable time.

In dealing with individual privacy and potential crime, prevention is better than cure. Let us not wait until it is too late.

The writer is a Nominated MP and professor of information systems and business policy at the National University of Singapore. He is co-author of a survey on the economics of privacy.