**Yui Kee Computing Ltd.**

# Newsletter

August 2010

## Contents

## Predator Cooperation

*Allan Dyer*

In an opinion column titled, "Octopus isn't the only predator out there" in the South China Morning Post (10th August), Mike Rowse, search director of Stanton Chase International and an adjunct professor at the Chinese University of Hong Kong, takes a lenient view on Hong Kong's Octopus card privacy scandal. While agreeing with much of the column, I would like to dissect some points in detail.

The Octopus card is Hong Kong's rechargeable contactless stored value smart card used to transfer electronic payments. It was initially introduced for public transport payment in 1997, and it has spread to become a common form of payment for shops, car parks and vending machines. The privacy scandal broke in July 2010, when it emerged that an insurance company had received and paid for personal data of about 1.97 million Octopus users.

Mike Rowse's first point is that personal data of the majority of Octopus users was not sold, because Octopus never had it. A standard Octopus card can be bought over the counter, without providing any personal data, and used indefinitely. People can also sign up for a "Personalised Octopus" that recharges automatically from their bank account or credit card. Also, there is an "Octopus Rewards" scheme where people can sign up for discounts and special offers. It is the personal data of people using these two schemes that Octopus sold, Octopus simply did not have the data about the holders of the other 15 million cards in circulation. The users of Personalised Octopus and Octopus Rewards even agreed to the sale when they signed up - the terms and conditions do mention that the data may be transferred, though, as Roderick Woo Bun, Hong Kong's Privacy Commissioner for Personal Data pointed out, you would need a magnifying glass to read them.

Mike Rowse concludes his first point with, "And no one will know anything about you", but that statement is missing important issues about how computers can be used to sift through vast quantities of information, and correlate information from different sources.

Octopus data was used by the Police to crack the Causeway Bay acid attack case. Someone threw a bottle of corrosive liquid from a building onto a busy shopping street in Causeway Bay, injuring several people. Police found a bag containing another bottle abandoned at the scene. They studied CCTV from the nearest MTR (Mass Transit Railway) station, spotted the bag being carried out through the ticket barrier and matched that to the Octopus card used.

Checking the Octopus travel records, they located where the card was generally used, lay in wait and arrested two suspects, later releasing one.

This is an excellent example of good Police work, using the available evidence and technology to track down the perpetrator who might otherwise have stayed free to attack again. However, it also points out that Octopus keep travel records for each card indefinitely.

Another group that collect behavioural information are A. S. Watson Group (HK) Limited, via their "Money Back" card. Each card has a barcode that can be scanned at participating shops, and for each HK$5 spent, one point is awarded. Five hundred points can be redeemed for a HK$10 voucher. In effect, by signing up (providing my personal information, name, address, HK ID card number), allowing my every shopping decision to be tracked and identified, I can receive a massive... 0.4% discount. The card is immensely popular.

So, with this information, I would like to explore a couple of possibilities. I do not think that these are happening now, they are possibilities that we should consider when deciding what protection our privacy deserves:

A large protest marches from Victoria Park in Causeway Bay to the Government Offices in Central. A repressive, authoritarian Government takes the Octopus records and matches cards that alighted in Causeway Bay around the time the march started and boarded in Central around the time the march ended. Some marchers are already identified, by their use of a Personalised Octopus, or membership of Octopus Rewards. Others can be identified when they use their Octopus along with their Money Back card.

Hong Kong is regularly hailed as the world's freest economy. However, economists study the disruptive effects of information imbalance on markets. A shopping chain that can correlate individuals' behaviour: when you shop, what you buy at different times, how much you are willing to pay for it; can manipulate that behaviour. Already, supermarkets no longer price-label items individually, shelf labels can be changed quickly according to day or time of day. Perhaps one day we will have contactless "loyalty cards" that can be read by shelf labels as the shopper approaches, adjusting the prices accordingly. The advantages of higher profits for the supermarkets are obvious, the consequences for the economy could be disastrous. Mike Rowse is correct in his second point that we agree to this when we apply for the loyalty cards, but would we agree if there was transparency in the value of the data we are "selling"? Who would agree to a proposition, "we give you a 0.4% discount, and you give us the information that will allow us to make an extra (for example) $1000 profit from you"?

This is not to suggest there is a conspiracy to exploit and repress. These scenarios can happen if ordinary people do ordinary things: work for the good of their company, increasing its profits, or respond to information requests from officials. What we need is transparency and safeguards. Terms and Conditions that say, "we may transfer your information to our business partners" do not provide enough information to make a rational decision. Perhaps there should be transitive responsibility for information: if company A transfers your information to company B, then A remains responsible for what B does with the information. The Police should be able to use travel records to track dangerous criminals, but with judicial oversight, so that it is not used to identify political opponents.

The possibilities and dangers of the information society are still developing, even technology specialists cannot predict the results, but we need input from all sectors of society to guide it into a positive course.

**More Information**

[Octopus isn't the only predator out there (subscription required)](#)

# Trojans Implicated in 154 Deaths

Malicious software on the airline's central computer may have been a contributing factor in the crash of Spanair flight number JK 5022 shortly after tackeoff on 20 August 2008, according to Spanish newspaper *El Pais*. Only 18 of the 172 passengers and crew on board survived.

The crash happened a day after the aircraft experienced two problems, and shortly after a failed take-off attempt. The airline's central computer recorded technical problems and should have raised an alarm after the multiple problems. A mechanic and an airport maintenance chief are also being investigated and may face manslaughter charges. The plane took off with flaps and slats retracted, which should have been discovered in pre-flight checks by the aircrew, and caused a warning in the cockpit.

The tragedy seems to involve a chain of failures, and prevention of any of them could have prevented the crash. An investigating committee should complete its report by December.

## More Information

El ordenador de Spanair que anotaba los fallos en los aviones tenía virus
Trojan-ridden warning system implicated in Spanair crash

Suite C & D, 8/F, Yally Industrial Building

6 Yip Fat Street, Wong Chuk Hang, Hong Kong

Tel: 2870 8550          Fax: 2870 8563

E-mail: info@yuikee.com.hk

http://www.yuikee.com.hk/