

## **CODES OF PRACTICE STAGE 2 ISSUES**

### **Discussion paper**

#### **Smart card and facial recognition technologies**

Smart card and facial recognition technologies may offer one avenue for facilitating responsible gambling in our community.

A brief discussion of each of these technologies is presented in this paper. It is envisaged that stakeholders wanting to make a submission to the Authority on one or both of these technologies may wish to consider some of the information provided in this paper in their submission.

#### **Smart Card**

Card technologies are often suggested as a way people could systematically identify themselves when gambling so that their preferences could be catered to in a systematic way.

While systematic identification does not require a card (because people could do so simply by keying in an account number and a PIN) or a smart card (most banks issue simple cards with magnetic strips), most discussion has centered on smart cards because of particular technical advantages they have for the South Australian technical environment.

This is because smart cards include the capacity to store and amend a significant amount of gambler information, and for that information to be processed "on the card", without the need for the gaming machines to be connected to a central computer system all the time.

This technology would allow for the gambler to make a pre-commitment decision (which could not be changed while the person was gambling) and be reminded of it, or have it enforced while he or she was gambling. Examples of pre-commitment decisions include the fixing of maximum hourly, daily, weekly and monthly spending limits.

The technology would also allow self-excluded patrons to be more readily identified than by the present approach of sending out photographs.

In order for the technology to be substantially effective, gaming machines could only be operated after a card had been inserted, it would be necessary for every gambler to have a card, and there would need to be enough control of the issuing of cards to ensure that it was unlikely that a potential problem gambler would have access to more than one card.

There would also be a need for venues to be able to issue temporary venue-specific cards, subject to rigorous processes, to deal with the circumstances of people visiting from interstate or even people who had left their cards at home.

Cost issues include the need to issue a large number of cards (possibly as many as 400,000) and to install additional equipment in 600 venues.

#### *South Australian example – J-Card*

An example of a smart card with which stakeholders may already be familiar, is the J-Card. About 150 000 J-Cards have been issued in South Australia, with 90 of the approximately 600 operational gaming venues equipped for the J-Card.

The J-Card system currently operates as a loyalty system. Loyalty points are awarded for a player's turnover on gaming machines. The site controller (ie. central computer in venue) collects turnover information from the gaming machine with which the card is associated and updates the card. This communication is one way.

J-Card members can currently, through the cashier in a venue, use their card to set time and expenditure limits relating to their gaming machine play. For example, a player could set a limit of \$100 or 2 hours play per session. Upon reaching such limits a text message is sent to the terminal the card is in, telling the player that their limit is reached. The terminal can also be made to make a noise to signal the reaching of limits.

It is also currently possible to send harm minimisation messages to the terminal.

The current technology is also capable of sending messages from the site controller to the venue cashier and the card reader terminal. This might be beneficial for the barring process, which involves the barring of problem gamblers from specific venues. The system could be used to advise the venue cashier when card number xxx belonging to a barred person is inserted into the terminal of a gaming machine in the venue.

At present, the J-Card system cannot communicate directly with gaming machines and so, it cannot shut down machines. A shut-down card system is not available in South Australia at this stage.

For further information about the J-Card system, with particular reference to harm minimisation, refer to earlier submissions made to the Authority by Worldsmart Technology Pty Ltd (see: two submissions under *Codes of practice – relevant documents – Submissions for 11 December 2002 hearing* and *Supplementary submission following 11 December 2002 public hearing (all gambling industries)* at [www.iga.sa.gov.au/pubcons.html](http://www.iga.sa.gov.au/pubcons.html)).

#### **Facial Recognition**

Some stakeholders have raised the potential for facial recognition systems to increase the effectiveness of voluntary barring schemes with regard to identification of barred persons entering gaming venues.

Facial recognition systems (often termed “biometric systems”) are programmed to make comparisons on either—

- a one-to-one basis (ie. is the person in this picture that person?), referred to as *authentication*; or
- a one-to-many comparison (ie. does the person in this picture match anyone in this group), referred to as *identification*.

The complexities of the systems and programs required to facilitate these comparisons vary substantially. In all instances, a reference measure is acquired such as a photograph of a person, and this is later compared with a test measure such as another photograph or video image of a person.

In the case of *authentication*, the process is much simpler than *identification* as it requires the comparison of two data sets (ie. reference measure against test measure).

In *identification* however, the amount of data for comparison is extreme, which tends to result in a high error rate (ie. false rejection and false acceptance). An example of *identification* would involve the scanning of faces in a crowd (ie. the acquisition of test measures) and then comparison with data sets representing faces, such as for example, comparison with a database containing previously acquired sets of reference measures representing known criminals.

The most widely applied use of facial recognition systems has involved *authentication*. An *authentication* trial conducted at Sydney airport, involved Qantas flight crew placing their passports on a reader while looking into a camera. Through the use of a computer program known as SmartGate, the image in the camera (test measure) was compared to the image on the passport (reference measure). Whilst media reports suggest that the SmartGate system was 98% accurate, it has also been noted that the results may not necessarily be generalised to the general population.

Facial recognition systems have been criticised on the basis that many errors occur as a result of contextual changes (eg. changes in hairstyles, glasses and the wearing of disguises). However, advocates of facial recognition technologies suggest that contextual errors can be corrected by taking a number of photos from different angles or by programming the software to be more sensitive to certain aspects of faces such as the distances between the nose and eyes.

Australian evaluations of biometric technologies have focussed on the specifications of software and a discussion of compliance issues in accordance with Australian security standards (see: <http://www.dsd.gov.au/>).

No known evaluations of applications of *identification* technology have been conducted in Australia and real-life applications of the equipment appear to be rare. Media reports of a facial recognition trial involving *identification* in Tampa Florida were unfavourable, and reports suggest that the system failed to correctly identify one criminal. Meanwhile, millions of additional funds have been allocated to

continue assessing the reliability of the equipment used in the Sydney Airport passport verification trial.

Cost factors include the need for the reference images to be photographed in a particular and consistent way, and the installation of specific purpose equipment and fit-out in 600 venues. Some of these matters are dealt with in the submission made by Mr Phil Cheney for an earlier codes hearing and in the websites referred to in that submission (see: submission under *Codes of practice – relevant documents – Submissions for 11 December 2002 hearing* at [www.iga.sa.gov.au/pubcons.html](http://www.iga.sa.gov.au/pubcons.html)).