

# Chapter 7

## Technology options for pre-commitment

7.1 This chapter provides an overview of the technological options that could facilitate pre-commitment. It is clear from discussions the committee had with witnesses that there are a wide range of possible technologies. In some cases there were varying views on the advantages and disadvantages of particular options. There was also variation in the estimated costs associated with these technologies. These are discussed in further detail in this chapter.

7.2 Associate Professor Paul Delfabbro, Adelaide University, outlined the range of technology options that were available in his submission to the committee:

Many forms of technology can be used to facilitate cashless gambling as well as pre-commitment features. These include: magnetic cards, ticket systems, smart-cards, radio-frequency cards and integrated technologies that use combinations of technology.<sup>1</sup>

7.3 The features of these individual solutions are discussed in further detail below. Summary table 7.1 showing the main features of the technologies is provided at Appendix 4.

### Cards and other devices

7.4 In terms of card-based technologies, the main types for consideration are magnetic stripe cards, commonly used in banking, and smart cards with embedded digital chips:

To date, the use of player cards is the most common vehicle for the introduction of these play information and management systems. Typically, EGMs in gaming environments are equipped with a card reader providing access to a central server. The swipe of the card in the card reader links the player to their personal information, which can be accessed through the EGM. The cards themselves can resemble (in form and function) credit cards with magnetic strips or other devices such as USB keys and scan-tags that function with near-field radio frequency technology. Player cards that function as access keys to the central server can enable the player to use a range of self-monitoring and control features such as limit setting and timeouts.<sup>2</sup>

---

1 Associate Professor Paul Delfabbro, *Submission 9*, p. 4.

2 Responsible Gambling Council (Canada), *Insight 2009: Play information and management systems*, RGC, Canada, 2009, p. 4.

### ***Magnetic cards***

7.5 Evidence was presented to the committee about the use of cards with a magnetic strip (or mag-stripe cards) similar to those commonly used in banking and EFTPOS transactions, sometimes in conjunction with a PIN. The committee heard that some clubs already used magnetic cards in conjunction with loyalty schemes:

With new opportunities for 2012 the Victorian RSL network will be introducing a fully integrated loyalty system to our business which also has pre commitment functionality. It will include a members kiosk on entry, all point of sale registers and player interface on EGMS. This new system will fully integrate with our magnetic swipe membership card and will allow us to communicate, promote, track and monitor our members and their habits whilst in our Sub-Branches.<sup>3</sup>

7.6 The Victorian RSL detailed the advantages of a magnetic card for its members:

It provides a universal magnetic swipe card with personal identification number issued to every member

Has the capacity to limit or refuse access with the ability to track and monitor member activity and spend patterns

Allows self-regulation to become a practical reality rather than a theoretical ideology with one card across a wide area network which currently operates on limited functionality

In addition it allows members to feel a certain sense of self-responsibility when they enter our premises as information about them is recorded and kept on record.<sup>4</sup>

7.7 Mr Declan Martschinke, Maxgaming, gave evidence that magnetic cards are capable of supporting pre-commitment depending on the system and hardware used in conjunction with the card:

...it is all about how smart your system is rather than your interface. You can achieve exactly the same functionality by using a mag-stripe card. So, as long as you have a methodology within the wedge<sup>5</sup> itself to allow people to put details in and assign it to an account, you can use a magstripe card to do that.<sup>6</sup>

7.8 Associate Professor Paul Delfabbro, University of Adelaide, outlined some of the advantages of magnetic cards to support pre-commitment on EGMs, while also recognising the security risks attached with this technology:

---

3 RSL Victoria, *Submission 103*, p. 5.

4 RSL Victoria, *Submission 103*, p. 5.

5 More detail on 'wedges' is provided below.

6 Mr Declan Martschinke, *Proof Committee Hansard*, 3 February 2011, p. 12.

---

These cards have some advantages: they are cheap to make, can be easily replaced and can be issued with small cash values if players forget their own cards. Such cards are, however, less secure, can be easily damaged and can be swapped between players without [easy] detection. Several pre-commitment systems can be implemented using this technology.<sup>7</sup>

7.9 Regis Controls agreed these types of cards could be cheap, but pointed to some weaknesses with them:

...magnetic stripe card is vulnerable to misreads; the technology for reading and encoding data on a magnetic stripe card is cheap and easily obtained thus allowing for data to be easily copied and scanned for information allowing for fraud and ID theft. Also magnetic stripe cards are prone to wear and data corruption.<sup>8</sup>

7.10 Responsible Gaming Networks offered their view that magnetic cards are vulnerable to fraudulent use:

...the difficulty with simple magnetic stripe plastic cards is that players, and in particular problem gamblers, can share their cards and PIN numbers without risk. Previous independent research has been provided in this submission outlining this case. In addition simple magnetic cards can be easily skimmed or copied, as evidenced by recent bank card frauds. These types of cards are currently often used in gambling loyalty programs. Crown Casino uses simple magnetic stripe plastic cards for their Crown Club loyalty program<sup>9</sup>

### ***Smart Cards***

7.11 The committee was presented with an alternative to the magnetic strip card—the smart card. According to an article provided to the committee by the Gambling Impact Society (NSW):

A ‘smart card’ is any pocket-sized plastic card with embedded integrated circuits providing some limited memory and/or microprocessor capabilities when interacting with external card reading devices. They can be used for identification, authentication, data storage, and application processing. In gambling, these devices have been most commonly used as a Player Loyalty/Reward card and/or a debit card for cashless gambling. However, a few jurisdictions have used plastic cards and smart cards that enable gamblers to establish limits on their gambling behaviour.<sup>10</sup>

---

7 Associate Professor Paul Delfabbro, *Submission 9*, p. 4.

8 Regis Controls, *Submission 29*, p. 31.

9 Responsible Gaming Networks, *Submission 39*, p. 15.

10 Gambling Impact Society (NSW), *Submission 36, Attachment A*, Dr Robert Williams, University of Lethbridge, Canada, *Pre-commitment as a strategy for minimizing gambling-related harm*, pp 2–3.

7.12 Smart card technology offers a range of functionality that could be applied to pre-commitment. Dr Jennifer Borrell a gambling researcher outlined these functions her submission to the committee:

Smart cards could do lots of things (including collect market intelligence) but they might usefully: (i) enable gamblers to pre-set limits (while acknowledging that if someone is already 'hooked' they may not be so effective); (ii) facilitate the effectiveness of self-exclusion (as patrons would not be able to venue-hop or slip past staff detection), (iii) identify patterns of problematic gambling to identify 'problem machines' and 'problem venues', (iv) identify patterns of problematic gambling in individuals to inform interventions (e.g. as implemented by Holland Casino).<sup>11</sup>

7.13 Regis Controls detailed the information storage capabilities of a smart card:

By programming the integrated microprocessor (chip) a reader can recognise and authenticate the authorised owner of the Smartcard using a PIN, fingerprint or other biometric means; the identity information is securely stored in the chip. Smartcards are universally used in government, defence and corporate systems where secure identification, physical access, secure data access and valuable information need to be protected.<sup>12</sup>

7.14 In addition to these features, the capability of smart card technology to store and update player's personal information, player activity and pre-commitment preferences without the need for communication with a central server or database was noted. Mr Ian Donald and Mr Elik Szewach from Regis Controls offered their views on this:

Senator BACK—The only thing that is in the machine is a reader. Everything is on the card and the card does not transfer any data to the reader?

Mr Donald—Correct.

Mr Szewach—Also, the card is keeping track of the limit. So, if the network breaks down—with most other systems the limit is lost—the card continues to read the limit regardless of whether the network is there. Therefore, it is a true limit.<sup>13</sup>

7.15 Mr Robert Chappell, Independent Gambling Authority, SA, gave evidence about the capability of smart cards to incorporate cashless gaming as a method of pre-commitment and their ability to lock players out of an EGM once they had reached their limit:

---

11 Dr Jennifer Borrell, *Submission 109*, Attachment, p. 12.

12 Regis Controls, *Submission 29*, p. 6.

13 Senator Chris Back, Mr Ian Donald and Mr Elik Szewach, *Proof Committee Hansard*, 2 February 2011, p. 64.

---

A card reader could be built to accept something like this and the money for gambling could be on it. The card itself could know at what point it should stop feeding money into the machine. I could tell the card not to let any more money off it for another 12 hours, 24 hours, a month or whatever, and it would all be locked in here. There is the equivalent of a 386 computer embedded on the chip.<sup>14</sup>

7.16 He went on to outline how cashless smartcard gambling would avoid the need to re-engineer the machine:

...it is possible to remotely disable the machine within, give or take, \$20 of what is on the meter through controlling the gaming machine's access to the player's cash...If the money is on the card or is on the account or is delivered to the gaming machine through some account-based or card-controlled mechanism, then it is possible to implement a mandatory stop to the machine when a person reaches their voluntarily set limits without engineering the rest of the gaming machine environment.<sup>15</sup>

7.17 Mr Ian Donald, Regis Controls, advised that many EGMs were already fitted with smart card readers:

By the way, we have said in our submission that about 50 per cent are already smart-card enabled. If industry is complaining about the cost then how come they have fitted 50 per cent of EGMs—poker machines—with smart-card readers?<sup>16</sup>

7.18 Mr Declan Martschinke, Maxgaming, explained some of the additional capabilities of the smart card they produce, for example how it could be linked to a player loyalty scheme via a monitoring operator system. This is a feature of the Simplay cashless card system currently operating in Queensland on a voluntary basis:

The play on the machine is then tracked and they will earn loyalty points for their play. They can then use different facilities to redeem those points, whether that is at a kiosk or through the retail side of the business through a point-of-sale interface. So we have the loyalty system, which you can extend to the cashless and precommitment systems.<sup>17</sup>

7.19 He described the system in more detail:

...the value on the card is stored in a central system back at our head office. The interaction with the machines is then done by the card. When you put the card in the machine it recognises that you have enrolled in the precommitment and the cashless system. It will draw down money to the machine to be played and when the person finishes their session they either

---

14 Mr Robert Chappell, *Committee Hansard*, 1 February 2011, p. 24.

15 Mr Robert Chappell, *Committee Hansard*, 1 February 2011, pp 23–24.

16 Mr Ian Donald, *Proof Committee Hansard*, 2 February 2011, p. 57.

17 Mr Declan Martschinke, *Proof Committee Hansard*, 3 February 2011, p. 3.

hit the collect button or they pull the card out of the machine. Whatever credits are on the machine will then go back to the account...<sup>18</sup>

7.20 Mr Martschinke went on to describe how the Simplay system is flexible enough so that funds from the card could be used on other purchases inside the venue, even when the EGM limit was reached:

The funds that are stored on that card are still accessible to the person. Although they cannot play the gaming machines with those funds, they can then go over to a cashier facility and withdraw the money from that card so that they can use it for something else.<sup>19</sup>

### ***Radio Frequency Identification Devices***

7.21 The committee was presented with another alternative, the radio frequency identification device (RFID) or tag. Unlike magnetic and smart cards which require insertion into a card reader, RFIDs are simply swiped or waved across a reader. Associate Professor Paul Delfabbro described RFID technology in his submission to the committee:

RF technology involves small radio transmitters in a tag, chip or card that send encrypted information to a reader next to the machine. These systems are versatile and have higher security (e.g., Maxetag).<sup>20</sup>

7.22 Global Gaming Industries (GGI) described their RFID pre-commitment device, Maxetag, which is currently being trialled on a voluntary basis in venues in South Australia. This tag is issued to the player by the venue and records a player's pre-set limits. It is encrypted with an ID specific to the player and this is then recorded in a central database with the player ID number as the reference. Player activity is logged and stored anonymously with no link to the player's actual identity.<sup>21</sup>

7.23 To activate, the device is simply swiped/waved over a player interface module (PIM) located at the machine. It draws information from the system against the player's ID number, including the player's pre-set limits.<sup>22</sup>

7.24 GGI outlined the communication process between the device and the system:

When a limit is set to the PIM, it will send a message to the central server identifying the TAG/CARD and the required limit. This limit will be stored in an encrypted form in the central database with a reference index using the TAG/CARD exclusive number.<sup>23</sup>

---

18 Mr Declan Martschinke, *Proof Committee Hansard*, 3 February 2011, p. 4.

19 Mr Declan Martschinke, *Proof Committee Hansard*, 3 February 2011, p. 4.

20 Associate Professor Paul Delfabbro, *Submission 9*, p. 4.

21 Global Gaming Industries, *Submission 78*, pp 5–6.

22 Global Gaming Industries, *Submission 78*, pp 5–6.

23 Global Gaming Industries, *Submission 78*, p. 6.

7.25 Mr Scott MacDougall, GGI, went on to describe how the device allows for the setting of limits:

What happens is that as you tag on, or put your card into the device, it says, 'Would you like to set a limit?' You physically have to say yes or no, so you are making a conscious decision before you move forward and you push yes or no.<sup>24</sup>

7.26 The tag sends a warning to the player as they approach their limit, rather than stopping the machine when the limit is reached. Play can continue past the set limit:

So you set your limit, but it does not stop the machine or lock the machine when you reach your limit. It will give an audio warning and a visual warning, and every time you insert money after that it will keep warning you. It is like a seatbelt alarm. Eventually you put your seatbelt on, you would like to think, in this case.<sup>25</sup>

7.27 Mr Earle Rowan, GGI, described how their system is educational, rather than prohibitional:

This has led us to take a different approach altogether—that is, to step away from prohibitional systems, systems that actually control and limit people. The system we have on trial in South Australia at the moment is a system whereby an individual can set a limit at the gaming machine for that session of play. We describe it as an educational system. It is an attempt to educate people to gamble responsibly rather than to force them.<sup>26</sup>

### ***Universal Serial Bus (USB)***

7.28 Universal Serial Bus (USB) or a memory stick is a data storage device in common use with modern computers. Because of its high storage capacity a range of digital information can be kept on the device, including biometric data such as fingerprints.<sup>27</sup> It operates by inserting the USB into a port, that usually comes standard on computers and other electronic devices. Responsible Gaming Networks advised the committee USB devices have some advantages over other data storage options:

There is no central storage of a player's biometrics. They also have large enough memory to operate without the need for a central database of player gambling records, if so required. They also operate without the need to memorize yet another PIN number and they can read/write data 100 times faster than cards.<sup>28</sup>

---

24 Mr Scott MacDougall, *Committee Hansard*, 14 February 2011, p. 14.

25 Mr Scott MacDougall, *Committee Hansard*, 14 February 2011, p. 14.

26 Mr Earle Rowan, *Committee Hansard*, 14 February 2011, p. 12.

27 More information about biometrics is provided later in this chapter.

28 Responsible Gaming Networks, *Submission 39*, p. 16.

7.29 Responsible Gaming Networks outlined how a USB device could come with an in-built fingerprint scanner removing the need for a central database to store such data. The fingerprint would be stored on the device for later comparison with every subsequent use, preventing player identity fraud.<sup>29</sup>

7.30 The committee also heard that the USB standard which is ubiquitous across machines, would allow USB devices to be readily used across all forms of digital gaming without requiring the installation of a separate reading device or 'wedge' on the machine.<sup>30</sup>

7.31 Some witnesses outlined concerns over USB devices. Mr Ian Donald from Regis Controls expressed concerns regarding the cost of USB-based pre-commitment:

USB basically is overkill for purpose. It is a more expensive solution. You would only even consider it if you were going to go down the biometric route...<sup>31</sup>

7.32 He also suggested USB keys could be easily tampered with and biometric information stored within the device destroyed without detection:

It is very easy to overcome biometrics if you are a problem gambler, particularly if it is a USB. All you need is a screwdriver or a penknife and you can destroy the biometric. It is not impossible to do it with a smart card, but you can generally see if it has been tampered with and you can charge people accordingly.<sup>32</sup>

7.33 This would be less likely to occur with a smart card, according to Mr Donald:

...it is more evident on a smart card. You can give it to someone in the industry and they can tell that it has been tampered with. There are tamperproof smart cards. It is much harder with a USB. Also, you cannot put a photo on that.<sup>33</sup>

### **'Wedges'**

7.34 The committee heard that forms of pre-commitment that relied on hardware to read devices could require the installation of a 'wedge' or device onto EGM machines. The term 'wedge' is jargon used by some in the gaming industry to describe hardware that is installed on a machine post supply, for example in order to enable card-based pre-commitment. A range of other words were also used to describe the hardware modifications that could be required on pre-existing machines including Player

---

29 Responsible Gaming Networks, *Submission 39*, p. 14, 21.

30 Responsible Gaming Networks, *Submission 39*, p. 16.

31 Mr Ian Donald, *Proof Committee Hansard*, 2 February 2011, pp 54–55.

32 Mr Ian Donald, *Proof Committee Hansard*, 2 February 2011, p. 56.

33 Mr Ian Donald, *Proof Committee Hansard*, 2 February 2011, p. 65.



Interface Module (PIM), Player Tracking Module (PTM) and card reader. Mr Justin Brown, General Manager, Aristocrat, described wedges to the committee:

With Simplay and one of the Queensland examples, the ‘wedge’ refers to putting the hardware in the machine to take a card reader or attaching it to the machine. As to the cost effectiveness of that, we are certainly not privy to the entire business model, but we have observed the Simplay system and the other techniques that are there. The underlying requirement there is a system venue—infrastructure in the system, cabling, databases and member sign up.<sup>34</sup>

### ***EGM modification?***

7.35 Some witnesses suggested that a significant proportion of EGMs would need modification. Mr Ross Ferrar CEO of Gaming Technologies Association estimated some 25 per cent of current machines would require hardware upgrades, and warned this process could be complex. For example, he noted:

Any postsupply physical or electrical change to any gaming machine may void electrical safety and related compliance, could compromise operational integrity and should be retested and recertified.<sup>35</sup>

7.36 He added that the cost of complete software and hardware upgrades, retrofits and replacement of machines that could not be upgraded, could exceed \$1.55 billion.<sup>36</sup>

7.37 Not everyone agreed that upgrading of machines would be onerous or difficult. Mr Robert Chappell, Independent Gambling Authority, SA, suggested that it could be relatively straightforward:

I noted in Mr Ferrar’s submission on behalf of the Gaming Technologies Association that he thought that some machines in Australia could be adapted while others would have to be replaced; but even in South Australia, where we have the oldest fleet of gaming machines in the country, they all have a coin acceptor, and those boxes could all be replaced by something that accepted a card or was connected to some sort of account-based system.<sup>37</sup>

7.38 He added while it was technically possible to do the real challenge was coordination and an agreed set of standards:

What it requires is coordination. That has come out in many of the submissions before the committee in this inquiry. It requires coordination, it

---

34 Mr Justin Brown, *Committee Hansard*, 4 February 2011, p. 17.

35 Mr Ross Ferrar, *Committee Hansard*, 14 February 2011, p. 29.

36 Mr Ross Ferrar, *Committee Hansard*, 14 February 2011, p. 29.

37 Mr Robert Chappell, *Committee Hansard*, 1 February 2011, p. 24.

requires agreement and, at a minimum, it requires an agreed set of standards as to the way it is going to be done.<sup>38</sup>

7.39 He further argued that any hardware upgrades would be subject to an open tender process and the selected tenderer could be expected to achieve some economies of scale, if as would be likely multiple terminals were upgraded at once:

But the question was posed, 'Let's not say you are doing a venue at a time but you are actually getting the contract to do 13,000 terminals at once, would you achieve some significant economies of scale and would you be able to reduce the cost?' Two people, who were at the time advocating the adoption of some sort of smartcard solution in this state, were prepared to say that a number of around \$800 a terminal was a fair number.<sup>39</sup>

7.40 The costs of particular technologies are discussed in further detail later in this chapter.

## **Identification issues**

### ***Biometrics***

7.41 Biometrics is the electronic scanning and storage of highly personalised data, such as fingerprints or retina scans. It has been suggested that a full mandatory pre-commitment system would require the use of biometrics, in order to safeguard against fraud.<sup>40</sup> Fingerprints were the only biometric identifier raised with the committee.

7.42 The Independent Gambling Authority, SA, described biometric technology in its report into smartcard technology in 2005:

Biometric technology makes use of people's biological individuality to systematically distinguish between people and positively identify them. A core component of biometric functionality is the digitising of biological features, such as a fingerprint or the way a face is arranged. A piece of hardware "reads" the biological feature producing a digital record which can then be compared with similar digital records to determine a level of match.<sup>41</sup>

7.43 Responsible Gaming Networks quoted from Dr Robert Williams of the University of Lethbridge in Canada as stating that the use of biometrics was needed to ensure devices were not swapped or stolen by players wishing to gamble beyond their set limit:

A biometric identification system is needed. Some sort of identification system is needed so that all versions of the gambling format(s) within the

---

38 Mr Robert Chappell, *Committee Hansard*, 1 February 2011, p. 25.

39 Mr Robert Chappell, *Committee Hansard*, 1 February 2011, p. 36.

40 See for example, the submission by Responsible Gaming Networks *Submission 39*, p. 3.

41 Independent Gambling Authority, *Submission 33*, Attachment 1, p. 10.

jurisdiction recognize the individual and his/her preset limits. It is also important that this identity system be biometric, otherwise some people (particularly problem gamblers) will endeavour to use other identities/cards when their own limits have been met. Smart cards with PINs are an improvement over regular cards, but still do not prevent card swapping, borrowing, or selling. Unless the card is used for other important purposes, then some gamblers (or potentially venue staff) will give away or loan their PIN smart card to other players. A biometric system is also the best protection against underage gambling.<sup>42</sup>

7.44 Relationships Australia recommended the use of biometrics in pre-commitment:

Recommendation 3

We recommend that biometrics of some type (for example facial recognition, fingerprinting or iris image) be recorded at the time of registration and that biometric readers be installed at each EGM in order that accurate tracking can occur of each person's gambling activities and to ensure that those who have reached their limit do not use others' cards or devices to continue betting. Proper registration would also reduce the numbers of minors gambling.<sup>43</sup>

7.45 Others expressed doubts over biometrics. Mr Ian Donald, Regis Controls, presented evidence that installation of biometric readers at all EGMs would be expensive and ultimately ineffective:

For a number of reasons, about 12 per cent of the population do not have a fingerprint. They are too old or they have been engaged in manual work and it may have worn off. There is no wall on the end of their thumb. Biometrics are going to be a much more expensive solution. This is mainly because, if you have to maintain 197,000 biometric readers—which are complex pieces of equipment...it is going to be extraordinarily expensive. You are looking at something like five times the cost for biometrics. The only real advantage is that it would minimise—but not eliminate—card sharing...It does not eliminate card sharing. I can log on using my thumbprint and allow someone else to play and collect my winnings. So it does not eliminate it. It is an awfully expensive and very risk-challenging situation. I would say, based on my experience over the last 30 years, that there is more than a 60 per cent chance that a biometric scheme would fail in this environment.<sup>44</sup>

7.46 Mr Donald considered the possibility of integrating biometric recognition into smartcard technology if it was decided that biometrics were required:

---

42 Responsible Gaming Networks, *Submission 39*, Attachment 1, p. 10.

43 Relationships Australia, *Submission 72*, p. 3.

44 Mr Ian Donald, *Proof Committee Hansard*, 2 February 2011, p. 55.

...if you do want a biometric solution you can do that using a smart card. There are smart cards that have been around for 15 years that read your thumbprint as you hold it. The card chip has my thumbprint stored on it. If this thumbprint is the same thumbprint it tells the machine that it is okay to play. You do not need to put readers on every one of the 197,000 machines; it is on the card. It is a much cheaper solution but you will still get a high failure rate because people will hold it incorrectly.<sup>45</sup>

7.47 The Productivity Commission presented its view that although identification was the key to a successful pre-commitment system, this could be achieved without the use of biometrics:

Mr FRYDENBERG—We have heard a lot about privacy concerns with a mandatory precommitment system, particularly that in order to be effective you will need some form of biometric identifier. We have heard about black markets in cards from international experience and that being one of the unintended consequences were it to operate here. You would need to have some form of biometric identifier, and that may be through a smart card or a USB or another form...

Dr Lattimore—First of all, it does not need to be biometric. The issue is identification, and biometric would usually relate to things like fingerprints or eyes and so on. It merely has to be a robust approach to identifying people. Of course, we use those approaches in a range of official areas; passports or to have a post office box. Even if you want to get a mobile phone these days you have to demonstrate who you are. So it does not have to be biometric in approach.<sup>46</sup>

### *Committee view*

7.48 The committee explicitly rejects the use of biometrics for identity purposes. It agrees with the Productivity Commission and others that the identification requirements needed to prevent player fraud can be accommodated with less intrusive technologies. The identification system must record basic information only, such as name and address. The committee does not accept that a range of personal data need be stored in a national database; but acknowledges that some basic data will need to be kept (perhaps jurisdictionally) for verification purposes.

### **Recommendation 32**

**7.49 The committee recommends that a detailed solution for registration, identification and privacy be referred to the national regulatory authority for progressing.**

---

45 Mr Ian Donald, *Proof Committee Hansard*, 2 February 2011, p. 56.

46 Mr Josh Frydenberg MP and Dr Ralph Lattimore, *Proof Committee Hansard*, 15 February 2011, p. 48.

## Networked, device-based and machine-based systems compared

7.50 The advantages and disadvantages of network-based, device-based and machine-based systems were discussed with the committee.

### *Device-based systems*

7.51 Dr Charles Livingstone and Dr Richard Woolley described the advantages and disadvantages of networked and non-networked systems to the committee. A non-networked device-based solution was first outlined:

This solution would be based on a user-carried device with sufficient memory to record player activity, recognise time intervals, and require periodic re-validation for continued operation. It would also have a unique identifier and the capacity to interface with an internet server for re-validation purposes.<sup>47</sup>

7.52 They noted that all current EGMs would be capable of being retrofitted with player tracking modules (or readers).<sup>48</sup> A device-based solution would include the following, amongst others:

Able to store player pre-commitment data on user-carried device (e.g., smart-card, USB drive)

Able to store player use data on user-carried device

Capacity to require monthly ‘re-validation’ for:

- a) Compulsory viewing of player activity statement (using data carried by the device); and
- b) Check to ensure device not reported ‘lost’ or self-excluded
- c) note – irregular users need only re-validate prior to session, but device deactivated if not re-validated monthly or in advance of session.

Device to be issued subject to high integrity identity check (100 points)

Default parameters on device; may be modified by user via internet or venue based validation kiosk at periodic intervals (for increased limits) or at any time (for decreased limits)

Device capable of being de-activated for a specified period of self-exclusion (including via use of a ‘panic button’ integrated into player tracking modules, via validation kiosks, or the internet.

Capacity to record request for self-exclusion and refuse issue of device.<sup>49</sup>

---

47 Dr Charles Livingstone and Dr Richard Woolley, *Submission 26*, p. 9.

48 Dr Charles Livingstone and Dr Richard Woolley, *Submission 26*, p. 9.

49 Dr Charles Livingstone and Dr Richard Woolley, *Submission 26*, p. 9.

7.53 Dr Livingstone and Dr Woolley further explained that personal data stored on a card or USB device would not need to be stored centrally or networked; the only centrally stored data would record the issuing of the device:

This stage of the system would require player pre-commitment and activity data to be stored on a user carried device such as a USB or smart card, but would not require user data to be stored centrally. What would be stored centrally would be data about the issuing of devices – i.e., that individual X had been issued with a device numbered Y with parameter settings Z, that that device had not been reported lost, and that individual X had not requested self-exclusion.<sup>50</sup>

7.54 In order to prevent fraud, the device would require periodic re-validation:

The device would require periodic re-validation, preferably monthly, at which time a player statement would be generated (using data stored on the device)...Re-validation would be refused if the device had been reported lost or if the individual had requested self-exclusion.<sup>51</sup>

7.55 It was also explained that a device could be supplied with default limits, which the user could decrease at will:

Devices would be supplied with default limits set at modest expenditure levels. Users could decrease limits at any time.<sup>52</sup>

7.56 Any changes the player wanted to make to their limits could be done via the internet or at kiosks:

This would be an internet based system accessible via users' personal computers in the privacy of their home or at kiosks located at venues.<sup>53</sup>

### ***Networked systems***

7.57 A second option, the networked solution (sometimes referred to as system-based) was also explained to the committee by Dr Livingstone and Dr Woolley:

This solution would expand the capability of the system described above by networking player tracking modules.<sup>54</sup>

Increased functions would include:

1. Support real-time collection of player data
2. Capacity to monitor use and provide real-time warnings of potentially problematic patterns of use.

---

50 Dr Charles Livingstone and Dr Richard Woolley, *Submission 26*, p. 9.

51 Dr Charles Livingstone and Dr Richard Woolley, *Submission 26*, pp 9–10.

52 Dr Charles Livingstone and Dr Richard Woolley, *Submission 26*, p. 10.

53 Dr Charles Livingstone and Dr Richard Woolley, *Submission 26*, p. 10.

54 These modules are essentially the readers or player interface modules that would need to be installed on the machines.

3. Exclude use of 'lost' or stolen devices in real time.

4. Monitor user limits, and the extent to which users achieve limits.<sup>55</sup>

7.58 A networked solution would allow for real time data collection, and would only require a magnetic stripe card capability. But there would also be disadvantages, as they explained:

Thus the principal advantage of a networked solution would be real time data collection and all associated benefits of this, including capability for player tracking software to be utilised. A fully networked solution could also operate without the need for smart devices, relying instead on a less sophisticated access card (e.g., a mag-stripe card only). However central data storage would be required in this case with associated privacy concerns arising.<sup>56</sup>

7.59 Dr Livingstone further elaborated in his evidence to the committee:

...some industry sources have suggested that the cost of introducing a successful precommitment system would be exorbitant because it would require networking of all available machines, leading to the need to withdraw half of the available stock of machines from the market and replace them and so forth at substantial expense. In fact this is not correct.<sup>57</sup>

#### *Jurisdictional or national network?*

7.60 The committee heard differing views on whether a network should be jurisdictionally based or national. Barriers to a nationally networked solution were highlighted to the committee. These include different technical standards operating across jurisdictions<sup>58</sup> and many different communication protocols to enable monitoring.<sup>59</sup> One estimate the committee received was that there were nine different communication protocols currently in use across jurisdictions.<sup>60</sup> The Productivity Commission reported six protocols, differing in age and complexity.<sup>61</sup>

7.61 Ms Louise Sylvan, Productivity Commission, noted:

One of the concerns at the moment is that the standards are quite variable across the states and territories. Our use of the term 'adaptive technology'

---

55 Dr Charles Livingstone and Dr Richard Woolley, *Submission 26*, p. 10.

56 Dr Charles Livingstone and Dr Richard Woolley, *Submission 26*, p. 10.

57 Dr Charles Livingstone, *Proof Committee Hansard*, 2 February 2011, p. 31.

58 More details on technical standards is provided later in this chapter.

59 Monitoring is undertaken to determine how much taxation is to be levied.

60 Mr Des Crowe, Australian Hotels Association, *Proof Committee Hansard*, 15 February 2011, p. 3. Also see Clubs Australia, *Submission 47*, p. 18.

61 Productivity Commission, *Gambling*, vol. 2, Commonwealth of Australia, Canberra, 2010, p. 19.14.

means you have a base set of standards, but the implementation of that in different jurisdictions could in fact be different.<sup>62</sup>

7.62 A national network could circumvent issues around players moving across borders in order to avoid their limits, according to Mr Mathew Rowell, Relationships Australia:

If it were not nationally networked and it was just jurisdiction by jurisdiction, naturally you would not have the national lens through which to look at the patterns and behaviours that accompany activities on gaming machines, but you also leave yourself open to stuff about being able to cross borders—the complexity of having to sign yourself up in another state, for example.<sup>63</sup>

7.63 Relationships Australia (SA), agreed that moving to a national network could address cross-border issues:

...there are numerous examples of towns/cities edging state borders where a gambler would have minimal difficulty crossing the border to gamble once selected limits have been reached. This may provide a basis for extending the reach of networked machines to nationwide over time.<sup>64</sup>

7.64 Others were not convinced of the need for a national network, as the following exchange shows:

Ms Law—Some of the borders, I guess, will be a problem, but I think it would mostly be a small area of Queensland and New South Wales and perhaps a small area of New South Wales and Victoria. We are not talking about the whole of the country.

Senator BILYK—You do not think there needs to be a national—

Ms Law—Not in terms of the border issue. If we want to, we could look into a national computer system or we could make it a state based computer system.<sup>65</sup>

7.65 The Productivity Commission argued that if a standard technology upon which jurisdictions could then build their individual pre-commitment systems were adopted, this would be the most cost effective approach:

The technology should be standard across Australia. That benefits industry. It is the most cost effective way to do it. Once you introduce this new technology, individual jurisdictions can implement different measures.<sup>66</sup>

---

62 Ms Louise Sylvan, *Proof Committee Hansard*, 15 February 2011, p. 45.

63 Mr Mathew Rowell, *Proof Committee Hansard*, 18 February 2011, p. 17.

64 Relationships Australia, SA, *Submission 67*, p. 2.

65 Ms Margie Law, Anglicare Tasmania, Senator Catryna Bilyk, *Proof Committee Hansard*, 18 February 2011, p. 8.

66 Mr Robert Fitzgerald, *Proof Committee Hansard*, 15 February 2011, p. 45.



---

### *Wide-area Networks and border areas*

7.66 As noted, a jurisdictionally-based network system could cause problems around border areas. Mr Tony Toohey, eBet, suggested an alternative solution to this potential problem—a wide area network:

We can and do run wide area networks. Currently if there is a club group in New South Wales that may have three or four clubs in their group, geographically apart, we would run a wide area network between those, where it is one central membership database...you might take an LGA, local government area, approach. It is very easy to link those venues.<sup>67</sup>

### *Monitoring Operator Networks*

7.67 Mr Declan Martschinke, Maxgaming, outlined the possibility of linking venues to a pre-commitment system via the current monitoring operator networks that have been already established. A monitoring operator collects data, usually for the purposes of taxation. By linking the system into the monitoring operator network, it is argued that the process of establishing pre-commitment could be simplified:

Because they are already connected to the machines, they can send messages, they can disable machines and they can do all sorts of things...what you have got is the ability for the monitoring system to at a central point capture all that information and then report back on things like how many people hit their limit, how much the limits were set at and all those sorts of things rather than have a machine-gun approach where you have so many different operators operating their systems.<sup>68</sup>

7.68 The Productivity Commission outlined the possibility of a third party holding data on player's gaming sessions, a role that is currently performed by licensed monitoring operators:

Currently there is monitoring undertaken by private companies like Odyssey Gaming and Maxgaming. They would be quite acceptable parties to hold data, and the main reason they would hold data is if you lost your device it would effectively be listed on the database. But it would not be something that would be open to private parties to use for any purpose. It would be a bit like a bank system which holds a record of your account; I cannot go and look up your account and nor could government.<sup>69</sup>

### *Machine-based solutions*

7.69 A third option is a machine-based solution, whereby individual EGM machines in a venue perform the main pre-commitment functions such as retaining information on player limits. Mr Justin Brown, Aristocrat, outlined the key differences

---

67 Mr Tony Toohey, *Committee Hansard*, 14 February 2011, p. 47.

68 Mr Declan Martschinke, *Proof Committee Hansard* 3 February 2011, p. 7.

69 Dr Ralph Lattimore, *Proof Committee Hansard*, 15 February 2011, p. 48.

between machine-based pre-commitment and other systems (device or network/system):

A system based solution is generally limited to a venue. It involves a card that is connected to a localised database of members. You need to be a signed up member and use your card in the machine. That is what we refer to as a system based solution. 'EGM based' means that every player, on every machine, has the option to set a time limit and a loss limit on the screen. It is not card based; it is not for card users only; it is software in the machine. You might be familiar with PID<sup>70</sup> screens in some markets which bring up an information display. It would be an alternative information display that the player could activate and set.<sup>71</sup>

7.70 Mr Brown also discussed with the committee the software options for machine-based pre-commitment, as being an alternative to replacing all current machines:

...the solution we are talking about would be applicable in most machines in a software-only change, so the new machine would not have to be purchased by the venue. Software-only is a game change—converting the game. The new software would have the EGM opt-in solution built into it, and the pricing for that change, taking into account market fluctuations, is around \$3,000 as a baseline for the product. So a range of the machines out there would be what we would term technically obsolete and would need to be replaced, but the majority of the machines—and this is subject to a technical order—would be capable of being upgraded via software, not an entire machine purchase.<sup>72</sup>

7.71 Mr Trevor Croker, Managing Director, Aristocrat, argued a machine-based system could lower costs particularly for smaller venues:

In our view, an appropriately designed machine based solution is the most workable in assisting problem gamblers with preserving individual privacy and choice. It could also be available on each machine regardless of whether an individual player was a member of a venue based card program or irrespective of any loyalty based hardware or software that may be used in the venue. Such an approach minimises infrastructure costs for many smaller venues that might otherwise be required to install significant networks—for example, to support card based precommitment systems.<sup>73</sup>

7.72 The committee viewed a demonstration of a prototype machine being developed by Aristocrat during a site visit at Aristocrat in North Ryde NSW. It is designed to come standard with a selected range of safe gambling features:

---

70 Player Information Displays.

71 Mr Justin Brown, *Committee Hansard*, 4 February 2011, p. 16.

72 Mr Justin Brown, *Committee Hansard*, 4 February 2011, p. 8.

73 Mr Trevor Croker, *Committee Hansard*, 4 February 2011, p. 2.

---

Aristocrat has already been working on a prototype of such a machine incorporating a player alarm clock that enables the setting of a time control, and a bank meter which allows a play to bank wins instead of accruing them in playable credits. This product will be entering a field trial in Queensland in the first half of 2011.<sup>74</sup>

7.73 One emerging machine-based technology which utilises remote sensing was described to the committee. Scientific and Technology Innovations put forward their proposal for a stand-alone sensing device placed near an EGM. This device is still in development phase and so is not currently available. They described how their device could be programmed to remotely sense harmful types play and send a warning signal to players, deterring them from continuing harmful play.<sup>75</sup>

## Other issues

### *Communication protocols*

7.74 As noted earlier, many different communication protocols currently exist across jurisdictions. Communication protocols govern the type of communication that occurs between the EGM and the monitoring authority. This allows for the monitoring authority to collect information such as expenditure, in order to determine the amount of tax to be levied.

7.75 Mr Earle Rowan, Global Gaming Industries, (GGI) explained the communication differences do present problems for the industry:

The main technical problem that any system faces is that there is no standardisation between states of systems. Every single state has a different system for operating, which poses an enormous problem in trying to control a gaming machine...<sup>76</sup>

7.76 Some protocols only allow for one-way communication, others allow for two-way communication. GGI outlined these:

- South Australia VLC - one way communication from machine to site controller (one port)
- NSW -ACT 'X' protocol – direct communication with each machine (multiple ports)
- NT, TAS, QLD, NZ – QCOM – bi-directional communications via the site controller. (One port)
- VIC - VLC – one way communication from machine to site controller (one port)

---

74 Mr Trevor Croker, *Committee Hansard*, 4 February 2011, p. 2.

75 Scientific and Technology Innovations, *Submission 4*, p. 4.

76 Mr Earle Rowan, *Committee Hansard*, 14 February 2011, p. 11.

(This is applicable only to Hotels and Clubs. Casinos use different communications standards). One port means that each Gaming Machine has only one communications port installed and it is dedicated to a single purpose, usually government monitoring.<sup>77</sup>

7.77 The NSW Government explained how monitoring currently operates in NSW:

All authorised gaming machines in NSW hotels and clubs are connected to a Centralised Monitoring System (CMS) for the purposes of calculating gaming machine duty payable by venues. Currently, the CMS cannot accommodate two-way communications with gaming machines in hotels or clubs...<sup>78</sup>

7.78 The Tasmanian government provided information to the committee on the communication protocols operating in its jurisdiction and the purpose of monitoring:

The Liquor and Gaming Branch collects, on a regular monthly basis, gaming machine turnover and expenditure information for gaming conducted at Hotels, Clubs and Casinos. This information, which can be collected at machine level is used by the Branch to verify the amount of tax payable by the Gaming and Casino Operators...The Gaming Operator utilises the Sentinel system which operates under the QCOM communications protocol to monitor and control gaming machines operating in Tasmanian Hotels and Clubs. The Casino operators utilise the Dacom system which operates under the Aristocrat Serial Protocol (ASP) for machines operating in Tasmanian casinos.<sup>79</sup>

7.79 Mr Declan Martschinke, Maxgaming, outlined the QCOM system which operates outside NSW:

In every jurisdiction there is a connection to the machine, so the differences come about through the way the machines interact with that system. In the QCOM protocol, which is used everywhere except in New South Wales, there is control over the machine whereby the machine is disabled unless it is talking to the system. In New South Wales the machines just play and then they send back information.<sup>80</sup>

7.80 Dr Ralph Lattimore, Productivity Commission, agreed there were issues arising from the different communication protocols used throughout jurisdictions:

The different jurisdictions have different capabilities. You have probably heard about the QCOM system in Queensland and so on. But some systems,

---

77 Global Gaming Industries, *Submission 78*, p. 2.

78 NSW Government, *Submission 110*, p. 7.

79 Tasmanian Gaming Commission, *Additional Information Received 5*, 24 February 2011, p. 2.

80 Mr Declan Martschinke, *Proof Committee Transcript*, 3 February 2011, p. 6.

such as that in New South Wales, are far less flexible because of their capacity for communicating backwards and forwards with the machines.<sup>81</sup>

7.81 He added:

It comes back to the point that we have been emphasising from the start, that it is critical to get a national approach to standards and systems that relate to gaming machines. So one of the first steps would be in relation to the monitoring systems and the protocols that are used for communicating between the machine and back to the monitoring systems.<sup>82</sup>

7.82 The issue of the current national standards and how they cause problems for industry is discussed below.

### *National technical standards*

7.83 The Australian/New Zealand Gaming Machine National Standard (the Standard) was introduced in 1998. The Standard's stated purpose is to 'set out the core requirements, common to all jurisdictions, for the design of gaming machines and games for operation throughout Australia and New Zealand and to guide testers in their testing for compliance with the Standard'.<sup>83</sup>

7.84 The Standard is prepared and updated by a National Standard Working Party drawn from the Australian and New Zealand gaming regulators and covers only technical issues. The Standard is not legislation and has not been enacted as such in any jurisdiction. Machines that do not meet the standard are not considered for approval.

7.85 The states and territories decide to what extent they adopt the core Standard and can specify amended or additional standards for their jurisdiction. Individual jurisdictional requirements are detailed in an Appendix to the core Standard. Where there is a conflict between any of the states or territories' requirements and the Standard, the jurisdictions' requirements have precedence:

It is the prerogative of each jurisdiction on the extent to which this document is adopted. Whilst it is intended for there to be no conflict between the "core" requirements and individual jurisdictional requirement, in the event of a conflict the local requirement for that jurisdiction overrides the Standard.<sup>84</sup>

---

81 Dr Ralph Lattimore, *Proof Committee Transcript*, 15 February 2011, p. 56.

82 Dr Ralph Lattimore, *Proof Committee Transcript*, 15 February 2011, p. 56.

83 *Australian/New Zealand Gaming Machine National Standard Revision 10.1*, 5 February 2010, p. 10, 1.1.2, [http://www.nt.gov.au/justice/licenreg/documents/gaming/gmns10\\_1.pdf](http://www.nt.gov.au/justice/licenreg/documents/gaming/gmns10_1.pdf), (accessed 9 March 2011).

84 *Australian/New Zealand Gaming Machine National Standard Revision 10.1*, 5 February 2010, p. 10, 1.1.4, [http://www.nt.gov.au/justice/licenreg/documents/gaming/gmns10\\_1.pdf](http://www.nt.gov.au/justice/licenreg/documents/gaming/gmns10_1.pdf) (accessed 9 March 2011).

7.86 Mr Robert Chappell, Independent Gambling Authority, SA, explained it further:

The Australia/New Zealand Gaming Machine National Standard is a document which translates the legal requirements in eight separate jurisdictions into a common form of words so that the industry sector can understand what it needs to do to comply in those jurisdictions. It is not a source of law; it has no legal status in the sense of being the authoritative source of what is legal or what is licensable. It is a cipher for the way the regulators apply the different statutory and regulatory obligations in various places. It is by its nature a document that responds to regulation and, if precommitment were mandated, I imagine the people who write it would very quickly introduce a chapter about how it works. But it is not itself a document that is capable of being amended to bring about any change to licensing.<sup>85</sup>

7.87 A number of witnesses commented on the shortcomings in the current arrangements around the Standard. Mr Scott MacDougall, Global Gaming Industries, outlined the fact that it is not truly national:

Industry has a national standard. We have been trying to implement a national standard but every state has different amendments.<sup>86</sup>

7.88 Mr Ross Ferrar, Gaming Technologies Association, outlined the issues for the gaming industry arising from the current Standard:

...there is a national standard which regulators assess gaming machines against. But each jurisdiction has an appendix, and in some cases, more than one appendix. The national standard document itself is just over 100 pages and there are a thousand pages of appendices. That gives you some sort of understanding of what you are dealing with.<sup>87</sup>

7.89 The existence of multiple standards across jurisdictions leads to multiple approval processes. Mr Ferrar suggested that:

A uniform national standard would be helpful in addressing the duplication of approval processes.<sup>88</sup>

7.90 The Productivity Commission also commented on the national standards in its 2010 gambling report:

...despite their name, gaming machine national standards are not really national standards, and the processes for their development and alteration are cumbersome and unnecessarily costly to industry...There is insufficient guidance given to gaming machine manufacturers about whether or not

---

85 Mr Robert Chappell, *Committee Hansard*, 1 February 2011, p. 30.

86 Mr Scott MacDougall, *Committee Hansard*, 14 February 2011, p. 24.

87 Mr Ross Ferrar, *Committee Hansard*, 14 February 2011, p. 31.

88 Gaming Technologies Association, *Submission 44*, p. 3.

---

particular gaming machine features are likely to obtain regulatory approval. While complete certainty is unattainable, greater clarity of the expectations of jurisdictions would reduce costs for manufacturers and venues.<sup>89</sup>

7.91 The Commission went on to recommend that:

Governments should reform gaming machine national standards by requiring consistency, unless the costs of variations can be justified by likely consumer benefits. Variations should be based on legitimate harm minimisation criteria and should take into account the costs that such differences impose on other jurisdictions, manufacturers and venues. Governments should jointly investigate the scope to rationalise current arrangements for accreditation and testing of gaming machines, to remove any unnecessary duplication of effort and cost.<sup>90</sup>

7.92 Further, the Productivity Commission spoke of the longer-term cost savings in introducing a technology which eventually would allow for remote adjustments to EGMs from a central location. This would provide 'both beneficial commercial aspects and beneficial harm minimisation aspects'.<sup>91</sup>

### *Committee view*

7.93 The committee agrees with the view that the current national standard is national in name only, is less than optimal and will require greater consistency in order to deliver greater benefits and certainty to industry. The committee is also concerned that the current standard does not adequately reflect consumer safety and harm minimisation principles. The committee agrees that a truly national standard would facilitate the transition to full pre-commitment.

7.94 However, it is also concerned that reaching technical uniformity should not delay the implementation of full pre-commitment. Recognising that timely adoption of harmonised technologies is unlikely to be achieved in the timeframe required, the committee recommends a phased approach be adopted. In the first phase states and territories continue to utilise their current protocols to implement mandatory pre-commitment features by 2014. In the second phase they move towards harmonisation of technologies. The third phase would see full implementation of uniform national technical standards. This phased approach would allow for early action to address problem gambling, while allowing the longer timeframe for technical challenges to be addressed.

---

89 Productivity Commission, *Gambling*, vol. 2, Commonwealth of Australia, Canberra, 2010, pp 17.30–17.32.

90 Productivity Commission, *Gambling*, vol. 1, Commonwealth of Australia, Canberra, 2010, Recommendation 17.5, pp 63–64.

91 Dr Ralph Lattimore, *Proof Committee Hansard*, 25 March 2011, p. 24.

### **Recommendation 33**

**7.95** The committee recommends a phased approach to achieving harmonised national standards. In the first stage, mandatory pre-commitment in all jurisdictions for players of high intensity machines is introduced by 2014. Jurisdictions may elect to use differing technological solutions to meet the national pre-commitment features.

### **Recommendation 34**

**7.96** The committee recommends that in phase two the national regulatory authority develop a timetable to move toward harmonisation of the Australia/New Zealand Gaming Machine National Standard, and adopt an agreed national standard reflecting consumer safety and harm minimisation principles.

### **Recommendation 35**

**7.97** The committee recommends that phase three would see full implementation of uniform national technical standards.

### **Cost of individual technologies**

7.98 The suggested cost of implementing mandatory pre-commitment technologies varied greatly depending on the solution and the nature of the interest group offering the advice. The top of the credible range is about \$3 billion<sup>92</sup> which is a little over half the sum lost by problem gamblers in a 12 month period.<sup>93</sup>

7.99 The committee also notes the view previously forwarded by the Independent Gambling Authority, SA, that the costs could be lower if an appropriate tendering process is applied.<sup>94</sup>

7.100 Mr Declan Martschinke, Maxgaming, outlined that costs may be borne by venues over time. For instance the cost of the Simplay system (card-based) incorporates a daily fee paid by the venue to the system suppliers who retain ownership of all components of the system including hardware and software.<sup>95</sup>

As an all-up fee, currently we charge venues for the hardware and the software to run cashless gaming and precommitment. It is around \$1.50 a day, which includes loyalty, cashless, precommitment, hardware,

---

92 The estimate range was between \$2.5 billion and \$4 billion. Mr Des Crowe, *Proof Committee Hansard*, 15 February 2011, p. 25.

93 The Productivity Commission reported that \$11.9 billion was lost on EGMs in 2008–09. They estimate that around forty per cent of losses (ie, \$4.8 billion) are generated by problem gamblers. Productivity Commission, *Gambling*, vol. 1, Commonwealth of Australia, Canberra, 2010, p. 2.1 and p. 5.33.

94 Mr Robert Chappell, *Committee Hansard*, 1 February 2011, p. 36.

95 Maxgaming, *Submission 19*, p. 6.



maintenance of the hardware—everything that they need to do...If it was a state-wide system and every venue needed to have online connectivity, there may be an additional charge of somewhere between \$5 and \$7 a day for the whole venue to have that online connectivity.<sup>96</sup>

7.101 In a supplementary submission provided to the committee Maxgaming indicated that the cost to implement a system such as Simplay would differ across jurisdictions:

If Simplay was to be supplied to other jurisdictions the price would obviously need to be reviewed to reflect the unique functional, technical and regulatory requirements within each jurisdiction, the changes required to existing Simplay functionality and the broader commercial contract/supply terms in that jurisdiction.<sup>97</sup>

7.102 Mr Robert Chappell, Independent Gambling Authority, SA, outlined their estimates of the costs of establishing card-based gaming readers on individual EGM terminals in SA:

The smartcard inquiry's report, which is annexed to the submission, talks about numbers in the region of \$1,400 to \$1,500.<sup>98</sup>

7.103 This cost per machine could be lower if more machines were upgraded. According to discussions the IGA had with Mr Hearne from Maxetag during the Smartcard inquiry this could be as low as \$800 per machine.<sup>99</sup>

7.104 Mr Justin Brown, Aristocrat, outlined the estimated cost associated with in-machine software to enable machine-based pre-commitment:

The \$25,000 figure Trevor noted represented a new machine... The price for the in-machine solution software change is down in the \$3,000, \$4000, \$5,000 range...<sup>100</sup>

7.105 Mr Ian Donald, Regis Controls, provided information about the estimated cost for an individual smartcard, which could vary depending on functionality:

CHAIR—What would be the cost to a not-for-profit organisation issuing them? What would be the cost of the card?

Mr Donald—The cost of the card would be anywhere between \$1 and \$5 generally. It would depend whether you wanted biometrics or not. That adds to the cost.

CHAIR—But a card with a chip would be between \$1 and \$5?

---

96 Mr Declan Martschinke, *Proof Committee Hansard*, 3 February 2011, p. 5.

97 Maxgaming, *Supplementary Submission*, p. 1.

98 Mr Robert Chappell, *Committee Hansard*, 1 February 2011, p. 36.

99 Independent Gambling Authority Tabled Document, *Additional Information Received* p. 62.

100 Mr Justin Brown, *Committee Hansard*, 4 February 2011, p. 8.

Mr Donald—It starts \$1 and goes up to \$5.<sup>101</sup>

7.106 He added that a card reader device could cost as little as \$5.<sup>102</sup>

7.107 The individual device in development by Scientific and Technology Innovation was estimated to cost around \$600.<sup>103</sup>

7.108 The Productivity Commission discussed the costs of implementing pre-commitment technology on pre-existing machines and proposed a staged roll-out could achieve some cost savings:

At the extreme, if you change the whole system overnight or in a very short period of time you would have to replace all of the machines, even some that were six months old et cetera, and the cost would be very high. A staged introduction means that, as Robert said, the normal replacement cycle would greatly reduce the costs of that.<sup>104</sup>

7.109 Many in the industry, including Clubs Australia, expressed concerns regarding the total cost of implementing a national pre-commitment system across Australia. They estimate this could reach \$2.5 billion.<sup>105</sup> The committee is cognisant of industry concerns over the cost of implementing a full pre-commitment scheme and this issue is further explored in chapter nine.

## **Conclusion**

7.110 The committee notes there are a range of technical solutions for implementing full pre-commitment. The particular features, advantages and disadvantages of each of these vary considerably, as does the cost. The committee is not comprised of technical experts and does not propose to recommend the adoption of a particular technological solution, device or system. We are technology neutral. It is possible that jurisdictions will elect to adopt different technologies, or a mix of technologies. The committee is not opposed to this, provided these meet the national pre-commitment features that this committee is recommending.

7.111 The committee agrees that there are a number of technical challenges that need addressing. Of these the committee considers the national standards are of paramount importance. These standards remain less than optimal for the purposes of pre-commitment and do not adequately reflect principles around consumer safety and minimising harms. A common set of technical standards would be preferable but is not essential for the introduction of pre-commitment. Nevertheless, work should be

---

101 Mr Andrew Wilkie MP and Mr Ian Donald, *Proof Committee Hansard*, 2 February 2011, p. 60.

102 Mr Ian Donald, *Proof Committee Hansard*, 2 February 2011, p. 58. This figure was also quoted in Regis Controls, *Submission 29*, p. 18.

103 Scientific and Technology Innovation, *Submission 4*, p. 7.

104 Mr Gary Banks, *Proof Committee Hansard*, 15 February 2011, p. 58.

105 Mr Peter Newell, *Committee Hansard*, 4 February 2011, p. 53.

undertaken on harmonising the standards and ensuring they better reflect such consumer safety and harm minimisation principles. However, implementation of pre-commitment need not be delayed while this work is undertaken.

