

8th November 2012

Committee Secretary
Joint Select Committee on Gambling Reform
PO Box 6100
Parliament House
Canberra ACT 2600

Dear Secretary,

We wish to make a submission to the Committee on the National Gambling Reform Bill 2012 recently presented to the Parliament of Australia.

We are an Australian company that has developed an international Award-winning pre-commitment system for the global gambling market. We have been granted a patent for our Australian-designed technology solution by IP Australia, and been granted patents by other international countries over the last 3 years. We have invested extensive Australian intellectual property and millions of dollars into R&D, proof-of-concept, prototype development and production of our pre-commitment system.

Our SAFETY NET pre-commitment system recently won a *TOP 20 Most Innovative Gaming Technology Products Award* at the Gaming Technology Summit in Las Vegas, Nevada, USA in May 2011. We are the first pre-commitment system in the world ever to win such an Award. One international Award judge stated in a recent edition of the US Casino Journal that *"every casino should have the system"*⁽¹⁾.

Our SAFETY NET system has the advantage of operating seamlessly on poker machines, the internet and smartphones – to deliver integrated pre-commitment, eliminate underage gambling and deliver effective self-exclusion for governments across all physical and electronic channels of communication.

Our CEO has been invited to speak as a global expert on pre-commitment at multiple international problem gambling conferences across North America, Europe and the Asia Pacific region over the last 3 years.

Independent academic researchers at the South Australian Centre for Economic Studies have reviewed our pre-commitment system. In their recent research report for the Australian Department of Families, Housing and Community Services and Indigenous Affairs titled "Problem Gamblers and the Role of the Financial Sector" the researchers describe the significant technological advances made with our SAFETY NET system and state that it will possibly result in it no longer being necessary to remove ATM and EFTPOS machines from clubs and hotels with gaming machines - *"Such a system would remove the issues relating to ATMs at gaming venues and reduce pressure on banks"*⁽²⁾ says the report.

A UK Gambling Commission report on *"Cashless and Card based Technologies in Gambling"*⁽³⁾ noted that our 'SAFETYNET' system is the only system in the world to provide a comprehensive consumer protection solution which can be easily used both offline, across multiple types of machines, as well as online over the internet (refer Table 4 page 36).

Our company recently received an AUSTRADE Export Marketing Development Grant Awards for international marketing of its SAFETY NET pre-commitment product.

We are currently in dialogue with a range of US Governments for the use of our technology in their recently legalised online gaming environment. Indeed the Governor of Nevada, Brian Sandoval, is currently keen to have our company set up a North American headquarters in Nevada - where shortly that state will be the first US state to deliver legalised online gambling to adults within its state borders.

Our Chairman has an intimate understanding of the gambling industry, being a former Executive General Manager of Corporate Affairs with Tattersall's in Victoria (operators of 13,750 poker machines) as well as an in-depth understanding of technology through his Bachelor of Science degree in nuclear physics.

We refer members of the Committee to our corporate website www.responsible.com.au and recent North American website www.RGNInc.com

It is in this context that we believe we can offer some valuable input into the current legislation before the Parliament of Australia, in order to deliver an effective and on-going pre-commitment environment for electronic gaming in Australia.

1. ILLOGICAL TO BAN ALL BIOMETRIC PRE-COMMITMENT SYSTEMS:

Firstly, it needs to be recognised by members of this Committee, and the wider Parliament of Australia, that biometrics has recently been established around the world as the most effective means to ensure compliance and delivery of reliable harm minimisation in the gambling industry.

It is astounding that at the same time the Australian Parliament is contemplating the banning of biometrics for pre-commitment (in this proposed National Gambling Reform Bill 2012), the rest of the world is discovering and deploying the significant benefits of biometrics in problem gambling harm reduction. For example, in Canada's largest state of Ontario their independent government appointed Privacy Commissioner has announced her support for the use of biometrics to stop problem gamblers being able to beat current self-exclusion system (see her recent Businessweek article as Attachment A and an independent Canadian media report as Attachment B).

The case for biometrics is strong and evidence-based.

In Nova Scotia, Canada, Omnifacts Bristol market research reported from their Canadian pre-commitment trial in the section on 'Card Sharing' that 37% of Nova Scotia gaming machine gamblers were sharing their pre-commitment cards by borrowing and/or lending, and that pre-commitment card sharing was directly correlated to PGSI score (Problem Gambling Severity Index score)⁽⁴⁾ - in other words problem gamblers were the highest users of borrowed plastic cards. Omnifacts reported that pre-commitment card sharing occurred for up to a week at a time and the borrower would take the card to several different locations to play.

The International Gaming Institute at the University of Nevada in Las Vegas report of this same Nova Scotia pre-commitment trial states *"In this instance, it appears that the most glaring example of gamblers "beating" the RGD (Responsible Gaming Device) was through substantial card sharing. While this is perhaps to be expected, this reality does render many of our research tools impotent, and we should pursue measures to address this problem. In the future, it may be that **biometric devices (that require, for instance, a thumbprint to start play) or facial recognition technology could take care of many of these challenges (in that they could eliminate the step where an identification card is needed)"***⁽⁵⁾.

It makes no sense for the Parliament of Australia to prescribe and permanently ban the new frontier of effective pre-commitment.

Eliminating biometrics through legislation as proposed in Clause 23(2) and 29(3) is a move against the current pathway and flow of global innovation in gambling harm minimisation; will restrict future options for future governments through such enshrined legislation; and in fact is unnecessary due to other protective measures already included in the current Bill. For example, the current Bill already contains sufficient controls to allow the Government of the day to decide which technologies and/or methodologies to employ for pre-commitment at both initial deployment, in any trial and at any future date through its inbuilt protective clauses 23(3) and 29(4):

We therefore strongly encourage this Committee to recommend the removal of Clauses 23(2) from the current Bill whilst retaining Clause 23(3), and the removal of Clause 29(3) whilst retaining Clause 29(4):

DELETE: 23 (2) A precommitment system for a State or Territory must not use biometric processes to identify a person who chooses to register through the precommitment system.

LEAVE IN: 23 (3) The regulations may:

- (a) prescribe a manner of identifying a person who chooses to register through a precommitment system for a State or Territory (subject to subsection (2)); and
- (b) prohibit a manner of identifying a person who chooses to register through a precommitment system for a State or Territory.

DELETE: 29 (3) A precommitment system for a State or Territory must not use 3 biometric processes to identify whether a person is registered for the State or Territory.

LEAVE IN: 29 (4) The regulations may:

- (a) prescribe a manner of identifying whether a person is registered for a State or Territory (subject to subsection (3)); and
- (b) prohibit a manner of identifying a person as registered for a State or Territory..

Clauses 23 (3) and 29 (3) by themselves give federal, state and territory governments a more dynamic policy setting capacity over time.

The Productivity Commission has never once in any of its multiple Reports on Gambling over the last decade ever recommended the banning of biometrics in the gambling industry. The Productivity Commission has always been technology-neutral in its recommendations, thereby allowing governments the ability to adjust to ongoing technology innovation. Legislation, once passed, lasts. It is good legislative principle not to restrict future options for future governments. Such a proposal allows the Government of the day to regulate as it best sees fit based upon the latest available technologies available now and into the future.

Our SAFETY NET system is actually the most privacy protecting, spoof-proof biometric system ever developed in the world. Unlike all other biometric systems it does not require central storage of a person's biometrics. The gambler is the only person ever to store or use their biometrics in their own personal storage device – no government, no gambling operator, no gaming machine, not even our company – ever stores a player's biometrics.

We acknowledge that some consumers in 2012 may have some privacy concerns regarding biometrics systems – based upon their current very limited understanding of advanced biometric systems such as developed in our global innovation. Accordingly in the alternative of the Committee not recommending the deletion of Clauses 23(2) and 29(3), then we ask this Committee to specify that any such ban should specifically apply to centrally stored biometrics. This can be achieved by adding the additional words “centrally-stored” when referring to any such banned biometric systems within this Bill:

Thus Clauses 23(2) and 29(3) would read in such an amended form read:

23 (2) A precommitment system for a State or Territory must not use **centrally-stored** biometric processes to identify a person who chooses to register through the precommitment system.

29 (3) A precommitment system for a State or Territory must not use **centrally-stored** biometric processes to identify whether a person is registered for the State or Territory.

It is interesting to note that even the Australian Hotels Association can support biometric ID Scanners for entry into licensed venues but not for use in controlling losses at poker machines as reported recently on 7 Yahoo News service: *"No-one from the Australian Hotels Association was available to be interviewed, but a spokesman said while the organisation is generally supportive of the use of ID scanners it is up to individual hotels whether they wish to use the technology"*.

The Victorian Government is also proposing to expand its use of video camera facial recognition technology to protect and assist consumers under personal threats after the tragic murder of Jill Meagher recently.

Both the Federal and State governments are also already using biometrics technology to identify individuals, and examples include:

- Dept. of Immigration and Citizenship Affairs, ACT– Biometric, Facial and Fingerprint recognition for applications (overseas and in country)
- Dept. of Immigration and Citizenship Affairs, - Use of Biometrics in Passports, E-gate in International airports.
- Dept. of Transport, Queensland – Biometric Driver's Licenses – Facial Recognition
- Dept. of Justice, NT – Banned Drinkers Registers – Facial and Fingerprint

Whilst the current Parliament may not wish to support biometric solutions, the current Parliament should not restrict the future options of future Governments to utilise the latest and most innovative and most effective means of reducing problem gambling available at any time in the future.

Furthermore, passage of the current National Gambling Reform Bill 2012 by the Parliament in its current form will significantly restrict our company's commercial ability to market our global Award-winning flagship pre-commitment product in our home country of Australia and any of its states or Territories. If we are restricted by law from providing our flagship products and services in this country we will have to seriously consider the future viability of maintaining our corporate headquarters in Australia.

We find it quite ironic that at the same time as governments around the world are speaking to us about our innovation and seeking our establishment in their countries, our own home country is attempting to ban the use of our Australian Award-winning innovation. Does the current Parliament wish to repeat the mistakes of past Parliaments who neglected Australian innovation and drove it off-shore?

Whilst the current Parliament may not wish to support biometric solutions, the current Parliament should not restrict the future options of future Governments to utilise the latest and most innovative and most effective means of reducing problem gambling available at any time in the future.

2. LOOSE REGISTRATION CONTROLS NEED TO BE FIXED:

Clause 23 (1) of the Bill specifies that a pre-commitment system *"may use a signature or photograph to identify a person who chooses to register through the pre-commitment system"*. This means a person can present themselves with a photograph of themselves and an associated false name, and potentially be under the age of 18 years and still register themselves for pre-commitment on gaming machines (particularly is such registrations are allowed outside a gaming venue).

The current Bill should be amended to require a *government issued* form of photographic ID at the time of registration for pre-commitment e.g. driver's licence (with photograph, address and signature), passport, or any other government approved forms of ID (through later regulation).

As stated earlier, independent research has shown that identify fraud is a problem in pre-commitment deployments around the world. Identity fraud could well negate the effectiveness of any preliminary trial of mandatory pre-commitment in Australia.

3. CURRENT LACK OF SANCTIONS FOR CONSUMER OR VENUE ABUSE:

The current Bill contains no offences or penalties for a consumer acting on behalf of someone else. As stated earlier it is well known from Canadian pre-commitment research in Nova Scotia that 37% of all players reported borrowing and/or lending their pre-commitment devices, whilst 50% of problem gamblers shared their pre-commitment devices. More importantly these same research findings clearly identified venue owners and venue managers were actively participated in encouraging and facilitating the sharing of pre-commitment cards of their venue patrons ⁽⁶⁾.

The current Bill has an extensive six (6) pages of sanctions for venue operators, gaming machine manufacturers and even ATM service providers (including Section 41 on Anti-Avoidance Measures) who breach the intent of this Bill. However, currently there are no sanctions in this Bill against venue operators, venue managers or consumers who abuse the intent of the pre-commitment regime (whether it be as part of a mandatory trial or otherwise).

Accordingly the Bill should be amended to include offences and penalties for people acting on behalf of another person(s) to fraudulently mis-represent their identity when using a pre-commitment system.

4. IMPLEMENTATION TIMEFRAME AND COST DECEPTIONS:

The reality is that a significant number of currently installed gaming machines in Australia can be readily and cheaply adapted to pre-commitment using universal *Player Tracking Modules* (PTM) loaded with pre-commitment software. No new gaming machines needs to be purchased to replace such machines. Once this Bill is passed these machines can be very easily and quickly converted to pre-commitment by the phase 1 timeframe of December 2013.

This means that at December 2013 the current Bill should require all newly manufactured, newly imported AND the current installed base of machines capable of being adapted to pre-commitment, to have pre-commitment. It makes no sense to have current pre-commitment capable machines placed on hold until December 2016 when conversion can simply and cost-effectively be delivered three years earlier.

This Committee should also not to be captured by comments being made by the poker machine manufacturers that it is not possible to deliver a pre-commitment trial within the government's current proposed timeframe. The reality is that we can deliver a pre-commitment system to the ACT well within 6 months of acceptance and for around only \$2,000 per machine. We formally advised ACT Clubs of this in writing way back in September 2011 as outlined in Attachment C of this submission.

I trust the Committee will see through the deceptions of Clubs Australia when they now claim (Clubs Australia slams cost of pre-commitment tech - Business Spectator AAP Release 2nd November 2012):

"It's impossible for them to replace the 198,000 pokies across Australia, at a cost of \$25,000 each, in less than four years, he said.

"A fairer method would be to require all new poker machines be equipped with voluntary pre-commitment, but to allow all remaining machines to be phased out of their natural life cycle," Mr Ball said".

5. INAPPROPRIATE AND UNREALISTIC DEFINITION OF NET LOSS LIMITS

When players establish their initial loss limits for a time period they typically consider the net amount of money they would be prepared to lose out of their pocket over such a period of time.

The current loss limit definitions in this Bill mean that a player's loss will technically be required to include their monetary losses out of their pocket PLUS their future potential losses of credits previously won on a machine, when establishing their net loss limit.

This means a player who wants to lose no more than \$100 out of their pocket in a 24 hour period, may win \$2,000 in instant credits at the start of his/her session, then lose \$100 in his/her next spin to be a net \$1,900 ahead for the session. However, at this stage he will be stopped playing as he/she has just lost his/her pre-designated \$100 "loss limit".

The current definition of player net loss will result in the creation of artificially inflated pre-commitment limits being set by players, so that they can continue to play with their credit winnings at any time. This will result in a significant detrimental impact on their overall financial well-being when they subsequently set artificially high limits so as to cover their potential credit winnings not being counted as real losses. In other words in the case above they may decide to artificially set their daily loss limit at \$2,000 to allow them to continue playing during times of credit wins – which in reality are very infrequent – thereby leaving their artificially high limits in place during periods of frequent losses.

This effect can be eliminated by removing 'credit spent' or 'credit won' from the current definitions of limit period expenditure and limit period winnings when calculating next losses.

6. INEFFECTIVE PRE-COMMITMENT/SELF-EXCLUSION MINIMUM TIME PERIOD STANDARD:

The current Bill's minimum standard of requiring only a 24 hour time limit setting period is too short a time to deliver effective pre-commitment or self-exclusion.

The Bill should at least require players to establish a fortnightly limit and a 24 hour limit as a minimum standard. The reality is that a fortnightly time limit is more realistic since it coincides with the frequency of most pay cheques and Commonwealth benefit cheques.

Furthermore the current Bill allows a player to set a self-exclusion limit of \$0. Under the current legislation this self-exclusion period is only required to last a minimum of 24 hours. Normal self-exclusion periods typically last many months (and typically are countenanced in multiples of years of time). Therefore self-exclusion limit periods of 24 hours are not going to deliver genuine self-exclusion periods for any effectiveness. In addition in any trial of mandatory pre-commitment there will be genuine players who wish to be excluded for the full 12 months of the trial and they should be provided with that capability without having the ability to reverse their decision on an ongoing 24 hour basis.

Committee members need to understand that this industry will attempt to capture its highest spenders, who are the problem gamblers and the self-excluded. This is not an industry where industry participants wish to deliver the safest and most effective products to its consumers. They simply wish to have the least effective harm minimisation product at the cheapest price.

7. CRITICAL ROLE OF THE PRODUCTIVITY COMMISSION IN DESIGN AND ANALYSIS OF A TRIAL

The current Bill may result in an independent body other than the Productivity Commission designing the trial and for the same or another independent body other than the Productivity Commission evaluating the trial.

Only at the end of this design and evaluation process is it proposed in the Bill that the Productivity Commission should undertake its final evaluation of the results of any trial. The Productivity Commission's role may only turn out to be to report a flawed design and flawed analysis of the results of a trial by the other independent body or bodies – resulting in worthless outcomes for future public policy development. No other independent Commonwealth body beyond the Productivity Commission knows as much about the gambling industry, its structure and its associated public policy issues. It needs to be given a more active role in any trial.

Such outcomes can be mitigated against by incorporating into this Bill that the independent Productivity Commission must be engaged in both the original design and original analysis of any trial (in co-operation with any other independent bodies).

8. UNACHIEVABLE PROMISED OUTCOMES OF THIS BILL

The 'Guide to this Act' within this Bill states on two (2) separate occasions that under this Bill players will be prevented from using gaming machines when they reach their limit: e.g.

*"If a person sets a loss limit and uses a gaming machine as a registered user, then, once the person reaches his or her loss limit during a limit period, **the person is prevented** from using gaming machines located in the State or Territory as a registered user for the rest of the person's limit period.*

This is a statement whose practical outcome cannot be guaranteed to be complied with as a result of the passing of this legislation.

The reality is that under this legislation any player who is registered and reaches their limit can simply remove their pre-commitment device from any machine and continue playing on any other machine in any gaming venue.

9. RISKS OF EXCLUDING CASINOS FROM ATM LIMITS:

It makes no sense to allow casinos an exclusion from the proposed ATM withdrawal limitation rules, for superficial reasons such as potential impacts on international tourism.

Domestic players will simply migrate away from hotels and clubs towards casinos due to the differential ATM cash access benefits offered by casinos. In a voluntary pre-commitment regime this will result in moving problem gamblers from hotels and clubs to casinos – thereby allowing the casinos to further gouge problem gamblers using their sophisticated player loyalty schemes and promotions.

It is ironic that major Australian casinos look to Asia as the gold-standard for their future development of integrated casino resort developments. The reality is that the two new integrated resort casinos in Singapore are required by Singapore national law to ensure that gamblers can be tracked and not exceed their financial pre-commitment limits across ALL forms of gambling – not just electronic gaming machines. Perhaps the Commonwealth Parliament of Australia might like to adopt an equivalent standard of national leadership for responsible gambling in our local casinos, rather than giving exemptions for exploitation to our local casinos. International visitors from many progressive countries already fully understand the risks of allowing unfettered access to cash in gaming venues.

In summary, we believe the above suggestions strengthen the proposed legislation and provide for a more effective delivery of pre-commitment for Australians.

We are happy to discuss any of the above matters.

Kindest regards,

Yours sincerely

Phillip Ryan
Chairman
Office: 03 93720191

email: p_ryan@responsible.com.au,
website: www.responsible.com.au
ACN: 140 181 960

*SAFETY NET - Awarded TOP 20 Most Innovative Gaming Technology Products Award
Gaming Technology Summit. Las Vegas, USA May 2011*

Bibliography:

- ⁽¹⁾ *US Casino Journal – The Technology Issue, May 2011 pp 18 -25*
- ⁽²⁾ *Department of Families, Housing, Community Services and Indigenous Affairs, “Problem Gamblers and the Role of the Financial Sector” by The South Australian Centre for Economic Studies, 2011 pp 14 - 15.*
- ⁽³⁾ *UK Gambling Commission “Cashless and Card-based technologies in gambling” Dec 2008 pp 36 - 38*
- ⁽⁴⁾ *Nova Scotia Player Card Research Project, Omnifacts Bristol, January 12th 2007.*
- ⁽⁵⁾ *University of Nevada, Las Vegas International Gaming Institute, Responsible Gaming Device Report 2007 page 48.*
- ⁽⁶⁾ *Nova Scotia Player Card Research Project, Omnifacts Bristol, January 12th 2007 pp 17, 41.*

Attachments:

- A. Business Week July 27th 2011 “It’s Possible to have both Facial Recognition and Privacy” Ann Cavoukian, Information and Privacy Commissioner of Ontario, Canada.
- B. “OLG facial scans to help gambling addicts” Canadian Broadcasting Corporation, November 26th 2010
- C. Email to _____, Clubs ACT from Phillip Ryan, Responsible Gaming Networks, dated 4th October 2011



It's possible to have both facial recognition and privacy

ANN CAVOUKIAN

Published Wednesday, Jul. 27, 2011 02:00AM EDT

Last updated Thursday, Sep. 06, 2012 10:22AM EDT

One of the most common forms of biometric identification is when our face is compared with a stored facial image, such as a driver's licence or passport photo. Facial-recognition technology automates this process.

First, a biometric "template," or representation of you, is generated from measurements of your physiological traits (in this case, the image of your face), and this template is retained in a database. Further samples from captured facial images may then be compared against this template - if there's a match, then you're identified.

Imagine a scenario where you're walking down the street or attending a sports event or shopping at a mall, and your photo is taken, identified, tagged and matched against a database of facial templates, without your knowledge or consent. This would be an affront to privacy that should not be tolerated.

Two key developments are making this scenario possible. First, sophisticated, high-resolution cameras in surveillance systems - and now conveniently embedded in our mobile devices - are allowing for the frequent capture of high-quality facial images "on the move." Second, software is now available that is capable of indexing vast numbers of photos, allowing for the creation of biometric databases. All of the photos we put on the Internet and social media, as well as other information about us that allows for the tagging of these photos, may now be accessible. Taken together, this makes it much easier to become automatically recognized, and far more accurately than before.

Your facial image and identity are your personal information. Being unique in nature, this biometric identifier can represent you in the digital world, and may be misused, lost or stolen, leading to potential matching, tracking, impersonation and other deceptive practices. Accordingly, there are significant privacy and security challenges to facial recognition that must be overcome to ensure that any "unanticipated" negative effects are avoided. Beware of unintended consequences!

The most serious is the linkage of your biometric template across multiple databases, for uses that were never intended. One's identity may now be routinely shared online by others, as well as one's personal profile and geo-location data. When facial recognition becomes widespread, your biometric template could be used to identify you in multiple databases.

Privacy is all about freedom of choice and personal control. We need to realize that the same technology that serves to threaten privacy may also be enlisted to its protection. This entails the use of Privacy by Design - embedding privacy directly into technologies and business practices, resulting in privacy and functionality.

But video surveillance and facial recognition need not be privacy-invasive. A system using biometric encryption is highly privacy protective, yet accurate and secure, leaving no digital trail of biometric templates behind. It's a solution that doesn't store the biometric template itself but rather a "private" template in which the biometric is irreversibly bound to a cryptographic key. It's currently being used by the Ontario Lottery and Gaming Corp.

The OLG serves millions of repeat customers a year, at numerous gaming facilities. For self-declared problem gamblers in Ontario, the OLG maintains a totally voluntary self-exclusion program that allows individuals to be removed from OLG facilities. This program is being carried out with the help of an innovative made-in-Ontario facial recognition system that *only* identifies possible matches with registered gamblers, while ignoring the vast majority of regular visitors, who remain anonymous.

Thanks to careful Privacy by Design planning, innovative use of advances in biometric encryption, and effective data stewardship, Ontario has a privacy-enhanced facial recognition system that can serve as a model for others around the world. Not only is it possible to have facial recognition *and* privacy, it's now a reality - and it's a win/win strategy.

Ann Cavoukian is Information and Privacy Commissioner of Ontario.

© 2012 The Globe and Mail Inc. All Rights Reserved.

ATTACHMENT B:

2/21/12

OLG facial scans to help gambling addicts - Technology & Science - CBC News

OLG facial scans to help gambling addicts

Last Updated: Friday, November 26, 2010 | 8:18 AM ET

By Sharon Oosthoek, [CBC News](#)

Ontario casinos and slots at racetracks are getting ready to introduce a facial recognition system for people who have identified themselves as gambling addicts, hoping to help them stay out of trouble.

In a project that has received the blessing of the Ontario Information and Privacy Commissioner, the Ontario Lottery and Gaming Corporation will install facial biometric video cameras at the entrance of all 27 of its slots rooms and casinos in 2011.

Starting next spring with the slots at its Woodbine Racetrack in Toronto, the OLG cameras will link to a system that alerts staff when someone registered with the service walks through the doors.

The system makes use of an emerging technology called biometric encryption that scans a person's face. When it picks out someone who has registered with the OLG service, it alerts staff and "unlocks" information provided by the registrant.

"The security team would be alerted and would talk to the person and remind them about the requirements and counsel them to leave," said OLG spokesman Rui Brum. If the person refused to leave, security staff would then issue a trespass notice, a move the person would have agreed to in advance.

While video cameras at the entrance will scan all customers, OLG said there is no danger of misuse of that information.

"OLG will not keep [video] records of anyone not self-excluded," said Brum. "They are captured and released immediately. If there is no match, they're released right away."

In addition, the system relies on an algorithm developed by University of Toronto engineer Kostas Plataniotis and his team that protects private information supplied by registrants.

Karl Martin, one of Plataniotis's former PhD students who helped develop the system, said the algorithm ensures there is no permanent link between the facial scan and a registrant's private data.

"If any data gets stolen, what they will not have is a bunch of personal information and biometrics data. They'll have biometric data that doesn't connect with anything. It's useless to anyone," said Martin, now president of KMKP Engineering, a University of Toronto spinoff company created to commercialize the system.

Provincial privacy commissioner Ann Cavoukian lauded the OLG facial recognition system earlier this month for making privacy integral, rather than an afterthought.

"This biometric encryption-based technology will offer dramatically improved privacy protection over simple facial recognition, without compromising any functionality, security or performance — the hallmarks of a privacy by design application," she said in a release.

Phillip Ryan

From:

To:

Sent: Tuesday, 4 October 2011 6:07 PM

Subject: SAFETY NET Pre-commitment system and associated Player Protection Key

Thank you for your time discussing the current pre-commitment environment in the ACT. As mentioned, our company would be interested in participating in any ACT trial of pre-commitment in partnership with Clubs ACT and the Federal Government.

In May this year our Australian designed and patented SAFETY NET pre-commitment system won an international *TOP 20 Most Innovative Gaming Technology Products Award* in Las Vegas, USA. Our pre-commitment solution eliminates card sharing by players which has been shown to be as high as 50% incidence amongst problem gamblers in overseas pre-commitment solutions (i.e. Nova Scotia, Canada). Our system also provides privacy protection to players. We utilize a biometric flash drive rather than a magnetic stripe plastic card.

We can convert current poker machines over to pre-commitment by using globally standard player tracking modules which cost less than \$2,000 per poker machine. This is significantly less than the \$15,000 per poker machine costs currently being quoted by poker machine manufacturers. We also believe we can have a trial up and running in the ACT by May next year.

I have an intimate understanding of the gambling industry, being a former Executive General Manager of Corporate Affairs with Tattersall's in Victoria (operators of 13,750 poke machines). I also have an in-depth understanding of technology through my Bachelor of Science degree in nuclear physics.

I refer you to our website: www.responsible.com.au for some additional information.

I look forward to further dialogue and feedback from you following your upcoming meeting with officials next Thursday.

Kindest regards,

Phillip Ryan
CEO & Managing Director
Responsible Gaming Networks Pty Ltd
GPO Box 20, Melbourne, Victoria Australia 3001

Direct Office: +61 3 9372 0191
email: p_ryan@responsible.com.au
website: www.responsible.com.au
ACN: 140 181 960

*SAFETY NET - Awarded TOP 20 Most Innovative Gaming Technology Products Award in Las Vegas, USA
May 2011*