Using Biometrics in Licensed Premises and Clubs – Are you protecting your patrons privacy and reducing risk of litigation?

If your organisation is a club or pub with a turnover greater than $3 million per year[1] and you are using, or considering, biometrics (i.e. fingerscans, iris scans, voice prints or facial scans), then your organisation must comply with the National Privacy Principles (NPPs) of the National Privacy Act.

POINT NUMBER ONE **Most pubs and clubs need to comply with the National Privacy Principles (NPPs) of the Privacy Act**

Biometrics are personal information just like a passport, a driver's licence, identity card or another identity document. If you copy or scan or collect any type of personal information from your customers you need to understand the National Privacy Principles.

POINT NUMBER TWO **Even if you are exempted, practise good privacy policy**

Even if you are exempted from the Privacy Act, you should still cover yourself by following the National Privacy Principles. Failure to properly deal with personal information may result in a person claiming damages from misuse of their personal information or prosecution under the Privacy Act

POINT NUMBER THREE **Have a valid business reason to collect biometric information**

If you collect fingerprints, driver licences and other personal details, ask yourself, if you really need to collect such details?

WHY IT'S IMPORTANT TO FOLLOW THE NATIONAL PRIVACY PRINCIPLES

Firstly, as a business owner or employee, you have a legal obligation to collect and manage that personal information appropriately.

Remember, if you are collecting any personal information, you are handling someone's identity. If it is a biometric you are collecting something very personal indeed. The way you handle that information is very important to a significant proportion of your patrons. Imagine, as customer, you have to give a pub your driver's licence and it is later stolen or lost or passed on to someone else who is not entitled to see or use it. The customer may well have grounds to sue for redress or complain to the Office of the Privacy Commissioner. The police may also be involved if that information is used to give someone else a false identity. This could potentially damage your reputation or worse, financially impact on your business.

[1] Please refer to the website of the Privacy Office to find out more: http://www.privacy.gov.au/materials/types/infosheets/view/6544

WHAT YOU NEED TO DO TO COMPLY

Below is a plain English version of the National Privacy Principles. Take a little time to look through them before you implement biometrics or any system that collects, stores or transmits personal information of your customers or employees.

NPP 1: collection

Describes what an organisation should do when collecting personal information, including what they can collect, collecting from third parties and, generally, what they should tell individuals about the collection.

NPP 2: use and disclosure

Outlines how organisations may use and disclose individuals' personal information. If certain conditions are met, an organisation does not always need an individual's consent to use and disclose personal information. There are rules about direct marketing.

NPPs 3 & 4: information quality and security

An organisation must take steps to ensure the personal information it holds is accurate and up-to-date, and is kept secure from unauthorised use or access.

NPP 5: openness

An organisation must have a policy on how it manages personal information, and make it available to anyone who asks for it.

NPP 6: access and correction

Gives individuals a general right of access to their personal information, and the right to have that information corrected if it is inaccurate, incomplete or out-of-date.

NPP 7: identifiers

Generally prevents an organisation from adopting an Australian Government identifier for an individual (e.g. Medicare numbers) as its own.

NPP 8: anonymity

Where possible, organisations must give individuals the opportunity to do business with them without the individual having to identify themselves.

NPP 9: transborder data flows

Outlines how organisations should protect personal information that they transfer outside Australia.

NPP 10: sensitive information

Sensitive information includes information such as health, racial or ethnic background, or criminal record. Higher standards apply to the handling of sensitive information.

In the meantime you should only collect information that is necessary for your business, if you do need to collect personal information you need to tell people;

- why you are collecting it
- what it will be used for
- who you will pass this information onto
- how your customer can gain access to the information you hold about them
- any law which means that the information has to be collected
- what might happen if the information is not given (e.g. no entry to the premises)

A full description of the National Privacy Principles is available from the Office of the Privacy Commissioner at http://www.privacy.gov.au/materials/types/guidelines/view/6582#npp3.

The Office has also released an Information Sheet (Private Sector) 30 - 2010: ID scanning in clubs and pubs http://www.privacy.gov.au/materials/types/infosheets/view/7074.

The Biometrics Institute has its own Privacy Code, which requires its members to deal with biometrics at an even higher standard than the Privacy Act. Of course these higher-level principles can be implemented by any organization, whether they are a member of the Institute or not. The Code can be found at: http://www.biometricsinstitute.org/displaycommon.cfm?an=1&subarticlenbr=8. and a checklist for its implementation can be found at: http://www.biometricsinstitute.org/displaycommon.cfm?an=1&subarticlenbr=188.

ABOUT THE BIOMETRICS INSTITUTE

The Biometrics Institute is an independent not-for-profit user group with currently over 100 member organisations including government departments, financial services institutions, health service providers and also vendors of biometric products and services. It is THE meeting place for organisations that have an interest in adopting biometrics to improve their business process and would like to share experiences and receive information and training in an informal environment.
The Biometrics Institute is based in Australia and represents organisations from Australia, New Zealand and beyond.

Contact details
Biometrics Institute Ltd
PO Box 576
Crows Nest NSW 1585
Australia
Tel. +61 2 9431 8688
Email: manager@biometricsinstitute.org
Web: www.biometricsinstitute.org