Timothy Pilgrim
Deputy Privacy Commissioner

Speech to

Biometrics Institute

Biometrics and Privacy

12.50 pm, 21 November 2007
Hyatt Hotel, Canberra

Biometric technology – good or bad for privacy?

What is interesting about biometric technology is that we tend to hear both that it is good and bad for people's privacy.

On one hand we hear that biometric technologies enhance privacy. This is well depicted in the film *Mission Impossible*, where we see top secret personal information of federal agents held in a room which only one person can enter and only after they have submitted to iris, fingerprint and voice recognition tests. Breaking in, as the movie title suggests, is a veritable 'mission impossible'. (It's just a shame that the ceiling vent in the room doesn't have the same protections!)

On the other hand we hear that biometric technology has the potential to invade our privacy. Two films come to mind which give us an eerie peek at a future without privacy. In *Minority Report* individuals are completely and continually trackable by ubiquitous iris scanning infrastructure. And in *Gattaca*, genetic information is used to determine the outcome of people's lives for them, frequently without their say and against their will.

How do such obviously divergent views on privacy and biometrics coexist?

The answer is: because biometric technology is what we make it. Biometric technologies are not inherently good or bad for privacy. They become good or bad for privacy depending on how they are designed, developed and deployed.

If we can create technology sophisticated enough to recognise a person by their gait or thumbprint or iris, then we can create technology sophisticated enough to enhance rather than invade privacy.

I believe this is an empowering view to take. And I think this is an important attitude to have when developing biometric systems.

Enjoying the benefits of biometric technology does not also mean we have to give up other freedoms or rights. Biometric technology has a lot to offer. Let’s make sure that those benefits do not come at too high a cost. Let’s take responsibility to develop biometric systems carefully so that they achieve their aims while protecting privacy.

What has changed?

In recent years, use of biometric technology has really taken off and a number of government departments have begun to develop new initiatives which incorporate biometric technology, such as the Biometrics for Border Control initiative and the Health and Social Services Access Card.

Of course biometrics have been around for a long time. The humble fingerprint has been guiding police investigations for decades and most of us have a bank card in our wallets with our signature on it.

So what has changed? Well, a lot. The growing sophistication of biometric technologies; the use of biometric templates; the ability to match or authenticate biometric samples with a high level of accuracy; the ability to store large amounts of biometric data and search it efficiently; the capacity to collect or authenticate biometrics without a person's knowledge; and so on – these conditions have implications for privacy.

Biometric information is sensitive information

Against this backdrop of technological advancement, let us consider the privacy implications of biometric information.

Well, biometric information is sensitive information. It is unique, high quality data about a person’s physical characteristics and for this reason it needs to be treated with care. When we collect biometric information from a person, we are not just collecting information **about** that person, but information **of** that person. Biometric information cuts across both information privacy and physical privacy. It can reveal sensitive information about us; our health, genetic background, age and it is **unique** to each of us.

Unique identification

It is this uniqueness which is one of the major advantages of biometric information in terms of its powers of identification. However, this same attribute can also create major privacy risks.

The availability of unique identifiers can enable greater surveillance and heighten the risk of identity theft. This is because, if a unique identifier is broadly used, it is much easier to link up information about a person from disparate sources. And if it is stolen or breached in some way, it can have a much bigger impact on the individual.

This is one of the difficulties that has arisen with the Social Security number in the US and also why in Australia we have clauses in the Data-Matching Act and the Privacy Act to limit the broad use of the Tax File Number.

In community attitudes research commissioned by our Office this year, 9 percent of respondents claimed to have been a victim of identity theft and 17 percent said they knew someone who had been a victim. 60 percent of respondents said they were concerned about becoming a victim of identity theft in the coming year.[1] If biometric systems are to be successful, they will need to allay people's fears about privacy risks such as identity theft.

Of course there are many options available to minimise the privacy risks associated with use of biometric technology. Systems can collect and use different

[1] Community Attitudes to Privacy 2007, Wallis Consulting, p 67 available at www.privacy.gov.au/business/research/index.html.

biometrics with different technology and take steps to control the interoperability of biometric systems.

Some biometric technologies are designed to handle replacement or modification of the biometric tag thus reducing its finality as a unique identifier. This is reportedly the case with some voice recognition technologies which can use a combination of biometric information about the voice and particular content (such as a password or number) read out by that voice. If something goes wrong a new password can be created.

These are a few of the many answers that biometric technology can provide us with to enhance privacy.

Identity management

When it comes to privacy and personal information handling, we at the Office of the Privacy Commissioner tend to talk a lot about ‘identity management’. Identity management means exactly what it says – how we manage our identities.

Biometric technology is one tool in the hardware of identity management – a very powerful tool at that. It allows organisations to confirm whether a person is who they say they are.

The thing that we must remember when using biometric technology is that people’s identities are sophisticated and multi-faceted, so the technologies that authenticate these identities must also be sophisticated.

As Mary Rundle, Fellow of the Harvard Law School has recently noted in her documentation of the 10 principles of identity:

> Identity is contextual. People have different identities that they may wish to keep entirely separate. An identity attribute that is relevant in one context […] perhaps should not be mentioned in another context […]. Information could be harmful in the wrong context, or it could simply be irrelevant.

All of us have different sides of ourselves that we share with different people. The side we show our families is different to the side we show our work colleagues, and this is different again to the side we show our doctor.

Privacy means managing those different sides of our identity in a way that allows us to feel comfortable. When personal information is linked or compiled into profiles, we limit an individual’s ability to operate under nuanced and multi-faceted identities. Identities are flattened into a single homogenous entity.

The problems with this have been well demonstrated recently by some individuals’ experiences with social networking sites, where people have posted photos or information about their social lives, only to have that information make an untimely reappearance when applying for jobs. Identities are not meant to be the same for all of our public interactions, and this is why we need to take care to cultivate an environment conducive to good identity management.

Biometric technology should, and indeed must, play a role in this. We must take care to ensure that a biometric identifier does not become an excuse to ‘flatten’ people’s identities and curtail their ability to maintain and present separate and different sides to themselves.

Identities are sophisticated and so biometric technologies must be the same.

Biometric information and the Privacy Act

Well, that's the big picture. I'd now like to focus on the law and law reform for a few moments.

The Office of the Privacy Commissioner enforces the *Privacy Act 1988,* which regulates the handling of personal information (that is, information privacy rather than physical or territorial privacy). However, as I said earlier, biometric information is interesting because it cuts across notions of both informational and physical privacy.

For this reason we need to take care when using it; for it is unique and more sensitive that other types of information.

Biometric information as sensitive information – what the ALRC is proposing

Recognising this fact, the Australian Law Reform Commission (which is currently reviewing Australia's privacy laws) has proposed that biometric information be classed as sensitive information under the Privacy Act. As it stands, the Privacy Act regulates the handling of personal information and sensitive information.

Personal information means

> information or an opinion […], whether true or not, and whether recorded in material form or not, about an individual whose identity is apparent, or can be reasonably ascertained, from the information or opinion.[2]

The Privacy Act also contains extra protections specifically dealing with what is termed ‘sensitive information’. Sensitive information is a sub-set of personal information and is defined as:

> (a) information or an opinion about an individual’s:
>
> i. racial or ethnic origin; or
> ii. political opinions; or
> iii. membership of a political association; or
> iv. religious beliefs or affiliations; or
> v. philosophical beliefs; or
> vi. membership of a professional or trade association; or
> vii. membership of a trade union; or
> viii. sexual preferences or practices; or
> ix. criminal record;

[2] s 6, Privacy Act 1988

> that is personal information; or
>
> (b) health information about an individual.[3]

The ALRC is proposing that

> ‘the definition of sensitive information be amended to include
>
> (a) biometric information collected for the purpose of automated biometric authentication or identification and
>
> (b) biometric template information.’[4]

For, in the ALRC’s words:

> ‘Biometric information shares many of the attributes of information currently defined as sensitive in the Privacy Act. It is very personal because it is information about an individual’s physical self. Biometric information can reveal other sensitive information, such as health or genetic information

[3] ibid.

[4] Proposal 3-6, Discussion Paper, Australian Law Reform Commission, Review of Privacy, 2007.

> and racial or ethnic origin. Biometric information can provide the basis for unjustified discrimination.'[5]

Currently in the Privacy Act, there are two sets of privacy principles; the Information Privacy Principles which cover the Australian and ACT Government public sector, and the National Privacy Principles which cover much of the private sector. Only the NPPs contain clauses that relate to sensitive information.

The ALRC is proposing that these two sets of principles be replaced by a single set. If this happens, it is possible that public sector agencies covered by the Act would have to comply with sensitive information provisions.

Continuing technological neutrality

A final thing I wanted to note in relation to the ALRC review process is the principle of technological neutrality. Currently the Privacy Act is technologically neutral, meaning that it regulates information handling without referring to specific technologies that facilitate information handling.

[5] Paragraph 3.170, Discussion Paper, Australian Law Reform Commission, Review of Privacy, 2007.

Our Office has argued for the continuing technological neutrality of the Privacy Act, and the ALRC has agreed with this idea in its discussion paper.[6]

Of course, technological neutrality does not mean that we want to bury our heads in the sand when it comes to technological change. It is our opinion that we can have technological neutrality of privacy laws while still having laws that are technologically relevant. We believe that technological neutrality allows the Privacy Act to be adequately flexible to accommodate technological change. What we don’t want is a privacy regime that goes out of date every time technology changes!

In order to accommodate particular technologies that create privacy risks which fall outside the scope of privacy legislation, we have suggested to the ALRC that the Privacy Act should provide for the Commissioner to make binding codes. This would give the Commissioner the power to respond in a timely manner to new technologies with specific privacy issues.

[6] Proposal 7-1, Discussion Paper, Australian Law Reform Commission, Review of Privacy, 2007.

Privacy principles

As I mentioned, the Privacy Act is principles-based in its application. This style of regulation lends itself well to technological change because the law does not deal with the minutiae of information handling, but the broader principles that organisations and agencies need to incorporate into their operations and activities.

A few of these principles are especially important to organisations or agencies using biometric systems, and I would like to touch on a few of these now.

Collect information fairly and, as much as possible, directly from the individual and with their knowledge. A concern associated with biometric technologies is that biometric information can be collected at a distance from the individual and therefore without their knowledge.

Use biometric information only for what you say you will. A temptation with rich high-quality data such as biometric information is to find additional uses for it to ‘make the most of it’ so to speak. This is a major privacy faux pas known as function creep.

Individuals have given you their biometric information in good faith, so you need to use it only for the purposes you said you would. Otherwise you risk undermining the individual’s trust and potentially interfering with their privacy. No one likes to feel as though they are losing control of how their personal information is being used.

Secure biometric information appropriately. As this is a sensitive form of information, you may need to take extra care to ensure that it is encrypted, securely stored, only accessible to authorised users and destroyed when no longer needed for the purposes under which it was collected.

Finally, systems should allow for **anonymity**. A concern with biometric technology is that because it can collect or authenticate a person’s identity without their knowledge, it could impinge upon a person’s ability to be anonymous. So think carefully about when it may be appropriate **not** to identify someone. If your call centre has voice recognition technology, allow individuals to opt-in to identification before you go ahead and identify them. Many individuals will be pleased with the convenience of this form of biometric technology, but you can be sure that they will appreciate being asked beforehand.

Biometrics Institute Privacy Code

The Biometrics Institute privacy code (approved by the Privacy Commissioner in 2006) builds on privacy principles in the Privacy Act to introduce some additional rules for organisations that use biometric technologies.

Under the Privacy Act, organisations and industries can develop their own privacy codes. The codes must be at least equivalent to the National Privacy Principles in the Privacy Act (which are the privacy rules that private sector organisations need to comply with).

The Biometrics Institute Privacy Code contains some additional principles which give us examples of how biometric information can be handled responsibly.

Some of the key points contained in those additional principles include

- ensuring that biometric information is encrypted immediately after collection

- destroying the original biometric information after encryption

- holding biometric information separately from other personal information

- de-identifying biometric information where practicable

- allowing participation of individuals in biometric systems to be voluntary

- obtaining free and informed consent of the individual concerned for any new uses of the biometric information (beyond those originally intended) and

- having a third party carry out audits of biometric systems

- doing Privacy Impact Assessments. [7]

[7] Biometrics Industry Code, available at www.privacy.gov.au/business/codes/biometricscode.doc

Trust

One of the drivers for the Biometrics Institute Privacy Code, as I understand it, was to raise the bar with privacy standards in the biometrics marketplace, to help to allay community concerns about privacy and biometrics and to help garner trust.

As the Biometrics Institute notes in the preamble to its privacy code:

> only by adopting and promoting ethical practices, openness and transparency can these technologies gain widespread acceptance.[8]

It may, or may not, surprise you to hear that government departments enjoy quite a high level of trust from the community. In fact, that trust has been growing. In the community attitudes to privacy research commissioned by our Office, 73% of people surveyed said they believed that government departments were trustworthy when it came to how they collected and used personal information. This is in comparison to 64% in 2004 and 58% in 2001.[9]

[8] Biometrics Institute Privacy Code, available at www.privacy.gov.au/business/codes/index.html#code.

[9] Community Attitudes to Privacy 2007, Wallis Consulting, p 18, available at www.privacy.gov.au/business/research/index.html.

Government departments cannot afford to be complacent. Agencies can lose this trust and their reputation overnight if they sustain a major breach of personal information or handle personal information poorly. Moreover, agencies need to be particularly careful to incorporate privacy principles into their operations as, in many cases, individuals may not have a choice about whether or not they participate in government systems or operations.

Biometrics for border control

It is clear then that trust will be the vital ingredient in any project that involves the uses of biometric technology. One good example is the Biometrics for Border Control initiative. Biometrics for Border Control is one of the most significant Australian Government led test cases for biometrics in practice, so it will be critical to get privacy right.

You will shortly be hearing from agencies participating in this initiative including Customs and DIAC, so I won’t spend too much time on this. However I do want to speak to you a bit about our Office’s involvement in Biometrics for Border Control.

Four agencies play a role and receive funding under this program and they are: Customs, the Department of Immigration and Citizenship, the Department of Foreign Affairs and Trade, and us – the Office of the Privacy Commissioner.

The inclusion of our Office in this initiative from the start speaks somewhat to the importance of getting privacy right in the Biometrics for Border Control projects. Privacy is not a side issue but something to build in from the ground up. For this reason, our Office is funded and will continue to be funded (until 2009) to audit the initiative and provide policy advice.

Good information handling that ensures accurate, reliable and secure data is imperative to the success of the project. Therefore, privacy – responsible handling of personal information – must be addressed at the outset and throughout the development of the initiative, not tacked on at the end or thought about after the fact.

Wrap up

In wrapping up, there are a few key points I'd like to leave you with.

When developing new biometric systems, think about privacy early – do not ‘bolt it on’ at the last minute.

I encourage agencies and organisations to do Privacy Impact Assessments (or PIAs) when embarking on projects involving biometric technology. A PIA is an assessment tool that describes the personal information flows in a project, and analyses the possible privacy impacts that those flows, and the project as a whole, may have on the privacy of individuals – it “tells the story” of the project from a privacy perspective.[10] PIAs help an agency or organisation to identify and recommend options for managing, minimising or eradicating privacy impacts.

Biometric technology has a lot to offer. And it is becoming more and more sophisticated by the day. Such sophisticated technology **can** and **must** manage privacy impacts carefully if it is to enjoy broad take up and success.

Thank you!

[10] Professor David Flaherty, Professor Emeritus, University of Western Ontario.