Biometrics Institute "Trans Tasman Standardisation for Biometrics" Conference
Wellington Convention Centre
1 October 2004

Privacy Commissioner, Marie Shroff

Thank you for the opportunity to speak to you today. I have been struck by the rapid and far-reaching developments in biometric technology and, in my new role as Privacy Commissioner, in their potential implications for the way personal information can be gathered, stored and disseminated.

We tend to think of biometrics as being a recent technological marvel. But biometric technologies are possibly the oldest method of establishing identity. Fingerprints were used in Babylon as seals on clay tablets recording business transactions. More recently, (but still a while ago) they figured in the courtroom climax of Mark Twain's *Pudd'nhead Wilson* where Wilson not only identified a murderer but also showed that two babies had been switched soon after birth and raised to adulthood in the wrong families. (One was the child of a noted judge and the other of a slave.)

The term biometrics has been taken into the public arena and has undergone a metamorphosis. In 1901, the first scientific journal addressing the study of measurement in biology was published – Biometrika. It is now one of the leading journals in international statistical research. Biometricians are scientists who study the application of statistical and modelling techniques to the biological sciences. And that is how my dictionary still defines biometrics – perhaps it needs updating? But to the media, and us, biometrics have become those small group of technologies that permit agencies to identify individuals unequivocally and often covertly. For instance, the use of facial recognition technology at the Superbowl in Tampa in January 2001 was headlined in the international press at the time.

I am aware of recent progress in the Australian context, where an industry-driven and developed draft biometrics code has been given to the Australian Federal Privacy Commissioner. It is pleasing to see a proactive approach towards regulation being taken by industry in this area. In all likelihood, the increasing prominence of biometric

technology and its application mean that if industry does not take steps to self-regulate, government, or regulators like myself, would step in and do so.

I recently attended the 26th International Conference on Privacy and Personal Data Protection in Poland. It is an annual gathering of all data protection and privacy commissioners from around the world. Biometric identification was one of the key sessions at the conference, and I believe one of the most well attended. If a reminder were needed that biometrics and privacy are not just an Australasian concern, this was it.

The panellists talked about the experience of biometrics in their countries, the various different biometric technologies and their very different maturities, possible uses, costs and limitations.

Certain privacy issues were noted as being raised by the use of biometrics, for instance:

- surveillance from afar through facial recognition
- movement tracking
- loss of anonymity in public spaces
- use of DNA beyond the purpose for its original collection
- use by both the private and public sector, encouraged by the decreasing cost of adopting the technology.

In terms of the data generated with biometrics, let us not forget that there is the biometric itself; the data associated with the biometric (such as place and time), and any additional data that is linked to the biometric from another source.

Other related discussion at the conference centred on the risk of function creep or scope creep once a biometric is collected. From my perspective, this is quite a fundamental concern, and one that is common to many proposals where technology is driving the advances. Are there limits that should be placed on the uses of the technology? If so, where should those lines be drawn and how should we best do that? Is legislation the answer, or should we defer to self-imposed controls by industry and developers?

Biometrics in passports were also discussed by the panel. They noted the potential it raised for passports to become international identification cards – comparable to the nationally-

based ID cards that countries like Australia and Canada have considered and put aside (at least temporarily) because of public objections.

Clearly, biometrics is a technology whose time has come. What these technologies are used for and how these technologies are implemented will determine their acceptability with the public at large. The technology itself is neutral, but its application may not be. The choice is in our hands: there is the possibility of both privacy invasive or privacy enhancing implementation and use.

The public and political climate for biometrics

My experience as Cabinet Secretary, at the heart of the government machine, has ensured that I am particularly aware of the swirling winds of public opinion and politics. Biometrics may be a relative zephyr at the moment, but I think it has the potential to catch momentum and strength. Gales of public and political interest and energy may work against the benefits that biometrics could bring. The link between ethics and science – for that is where biometrics sits as I see it – is a potent and provocative combination.

I recall the concern that the emerging science of robotics engendered some decades ago: we were all at risk of being caught in the thrall of a robot gone wrong: at the same time fascinated by the wonders of scientific invention and fearful of its capacity to get out of human control.

Developments in nuclear science; human-assisted reproduction; genetically-modified organisms and human genetic engineering have all generated fierce social and political debate. Do not for one moment think that biometric technology will slip by without catching the attention of some political parties and the wider public. How prepared are we to debate the pros and cons? What reassurance could we offer to the public? Where are the limits of the technology now – and in the future? Activities like the gathering you are having today can help to prepare the ground and, ultimately, assist in moderating the political winds.

Some of you will already be aware of commentators such as Roger Clarke, who have

vehemently voiced concerns about the possibilities of biometric technologies:[1]

> Biometric technologies are … extraordinarily threatening to the freedoms of individuals, variously as employees, customers, citizens, welfare-recipients, and persons-in-the-street. Yet the design of schemes that are substantially invasive of the privacy of the person, and of behavioural privacy, as well as of data privacy, is being undertaken by organisations in blithe ignorance of the concerns of the people they are intended to be inflicted upon.
>
> Biometrics technologies are being implemented so badly, and in such a threatening manner, that they need to be banned, until and unless an appropriate and legally enforced regulatory regime is established.

The views he expresses are strongly put and many might take issue with his interpretation. I do not necessarily see the situation as so dire. However there undoubtedly *are* risks associated with the use of the technology and there are startling levels of ignorance in the wider community.

Part of the appeal of biometric identification technologies is that they are tools we use instinctively from the day we are born. Babies can distinguish their mothers' faces and voices from their first days. We recognise friends at a distance by the way they move as well as their shape. Our first writing is usually our own name. These characteristics are an intimate part of our identity as individuals. Biometric measurement of faces, voices, signatures, gait, and shapes are all in use today. The capacity for this to generate a sense of fear, invasion or loss is obvious.

ID theft is reported to be increasing all over the world and recent articles suggest that it is becoming increasingly the crime of choice for organised crime. Biometric identification may help protect us from that but, conversely, if those technologies can be perverted to the use of crime, the results would be frightening.

Those at the leading edge of the technology's development and implementation do have a responsibility to look beyond today. Citizens, in New Zealand and elsewhere, deserve to

[1] Roger Clarke "Biometrics' Inadequacies and Threats, and the Need for Regulation" (2002) available at http://www.anu.edu.au/people/Roger Clarke/DV/BiomThreats.html

be informed and to be able to find digestible information that assists them to understand and assess the risks for themselves. Transparency and accountability are important when the issues have such widespread impact.

I can only support and encourage you to continue and expand the approach you appear to be taking – of informed awareness and measured development.

New Zealand context

So where does privacy fit in all this? Privacy is of course ultimately about individuals. Individuals are the building blocks of society. Each of us as an individual needs freely to form, develop and maintain our identity and sense of self; we need a personal safety zone, in order to provide that freedom.

New Zealand is in the fortunate situation of having some good basic protections in place with the Privacy Act. But what effect will the Privacy Act have on biometrics? In general terms, if the privacy principles were distilled down to their vital essence, they would involve two or three key components:

- openness
- fairness
- clarity of purpose.

Openness and transparency enhance the accountability of public sector agencies; and assist businesses by building trust with customers. Clarity of purpose is essential: why is there a need to collect personal information? What will the information be used for? Who will it be shared with? How long should it be kept? Answers to these sorts of questions will be apparent to an agency with a clear view of its purpose in collecting the information. Unnecessarily extensive, intrusive or opportunistic collections of personal information are not consistent with the privacy principles and may well fall outside an agency's lawful purpose.

Although biometrics is a new area, it is not fundamentally different from other examples of emerging technology. There is currently much interest in privacy matters. The major driver of this is scientific, especially information and communications technology

advances, with all their huge capacity to identify, collect, aggregate and match personal information about individuals. Concerns about the safety and use of individual information are therefore increasing, and increasingly justified. On the other hand, these developments are a major tool for government and business to improve efficiency, service and security. Experience has shown that the Act *can* cope with most of these developments, despite being drafted before the technology came on the scene.

Other legislation too, such as the New Zealand Bill of Rights, will be relevant in the protections it gives citizens against unreasonable search and seizure (section 21). This could have bearing upon the circumstances in which the biometric data could be gathered.

And, certainly, we need those protections. At no time have we had more:

- pressure to use privacy-invasive technology
- capacity to do so
- interest, as well as fear and concern from the public.

These are very powerful pressures; combined with the need of business to sell new products they have expensively developed, it is a potentially explosive combination. Many of you here today will remember the INCIS fiasco. There are lessons to be learned for the biometrics players from that; too far, too fast, too complex and your project can collapse, with attendant damage all round.

New Zealand Customs and Internal Affairs developments

Like many other countries with visa-waiver status for travel to the United States, New Zealand is in the process of incorporating a facial biometric identifier into each newly issued passport from October 2005 by way of a digitised photo on a microchip. You will hear more about that from other speakers later today. New Zealand Customs is also testing facial recognition software and exploring its potential uses as a border protection tool. I understand iris recognition is already in use in a joint effort by two Canadian federal agencies to speed up border crossing to and from the United States for frequent travellers.

These are examples of high-level systems with rigorous testing, but there are also smaller scale New Zealand examples, such as the school that introduced student fingerprints rather

than library cards for the issue of library books. The appeal of the biometric system is clear: the software was described as far more efficient than the old system of cards and typing in names. And it speeds up issuing.[2] We do not have stretch our minds to think too of the appeal of biometrics in the consumer context. Steven Spielberg's film *Minority Report* showed Tom Cruise's character being recognised by the technology and immediately being targeted with personalised marketing, based on his previous purchasing patterns. Consider too the possibility of electronically enabled fingerprint access to your house or apartment – which is potentially only a few steps away from your fingerprint being made available for sale on the Internet. Yes, it is fantasy – but the real world isn't so far away.

Whatever steps we do take into a biometrically-designed present or future should be measured and we should be using our guide ropes and safety nets. There are benefits to be gained from the technology without jeopardising other values such as privacy or personal autonomy or independence.

New Zealand will have to confront these issues – and sooner rather than later. Internationally, there is huge pressure to adopt compatible technology. Decisions and priorities will all but be determined for us unless we move forward and state our position.

I firmly believe that we have some key guiding pointers. The first might be that there is huge power for good, and huge power for misuse. We *need* controls and protections.

The second of these is that taking privacy into account is good for business. The requirements of the Privacy Act may have implications for the way a business deals with its employees and clients, but it also assists them. The Act is about fair information handling practices – and fair dealing and openness are good business fundamentals. Customers will choose with their feet and a business that plays fast and loose with their personal information will not flourish. A survey commissioned on behalf of the Office showed this to be the case.[3] Ninety-one percent of New Zealanders surveyed said that they would be concerned (including 79% very concerned) if a business they supplied their information to for a specific purpose used it for another purpose. Eighty-nine percent were

[2] "Thumbs up for fingerprint scheme" *New Zealand Herald,* 30 April 2004.
[3] UMR Research survey, 13-16 September 2001.

concerned (including 78% very concerned) if a business they did not know got hold of their personal information.

The third aspect is that citizens have real rights. Ensuring that new systems are consistent with those is not just a regulatory burden, it is simply a reflection of what each person is entitled to under law to ensure individual well-being. The Privacy Act is not special – it is part of a wide range of consumer and human rights protections which make New Zealand a good place in which to live.

Code-making power

So, what extra help or assistance can the Privacy Commissioner's office provide? I have been tasked with numerous functions and powers under the Privacy Act – some are generally used – conducting own motion inquiries; making public statements; drawing matters of concern to the attention of the Prime Minister; as well as considering complaints of breaches of the privacy of individuals. Any or all may be of use in the context of biometrics and their application.

A further specific function granted to me under the Act is the power to make codes of practice. These must be distinguished from voluntary, industry-driven codes. A code issued by me under the Privacy Act is enforceable, with the status of a regulation. (One of the checks upon the code is that it is subject to review by the Regulations Review Committee of Parliament.)

I do not suggest that this is something I would rush to do – nor that it would necessarily be the best or only solution. Developing and issuing a code is a resource-intensive activity for my small office, and would be especially so in an area such as biometrics, which is relatively new and also contentious!

Conclusion

In New Zealand we are early adopters of new technology. In 1879 Charles Darwin said

"the extent to which science is cultivated in New Zealand always excites my imagination." We will give almost anything a go and we are undaunted by new ideas and applications. This is good as long as we proceed with caution, take the user along with us, and listen carefully to their concerns – and are wary of "snake oil" salesmen. I hope and anticipate that we can find a proportionate response in which there is a culture of respect for privacy as well as an appetite for the new.

I would not pretend that there are several – or even a dozen – privacy "solutions" to hand that could deal with all that biometric technology could throw at us. Quite simply that is not the case. It will need creative thought and a careful approach. My office will, to the extent possible within our resources, assist where we can. A code of practice is one possible avenue. But successful strategies will need to involve industry, government, privacy advocates and citizens, as well as regulatory bodies.

I am sometimes asked whether it is now too late to protect our rights and our privacy. I believe that not all is lost. We do have the time, and it is vital that we get things right. It would be a pity if the effect of the small-time cowboys were to de-rail your well-planned efforts and seriously damage the future prospects of implementing biometric technology in a privacy-neutral (or even privacy-friendly?) way.

We are at a critical point in the developing use of biometrics. I look forward to working with you to put biometrics to use in a way which contributes to the good of New Zealanders.