

Privacy Law and the future debate for Biometrics in Corporate Security

Craig Horrocks, Clendon Feeney

This seminar investigates the effect of biometric authentication on our privacy rights as set out in the Privacy Act 1993 in light of the potential future of our organisational security in the use of biometric authentication.

This seminar will be an interactive session in which the speaker will set out initial propositions, describe 4 hypothetical scenarios and ask questions that relate to those scenarios. Attendees will be invited to debate the propositions and issues that arise in the seminar.

PART I: PRIVACY LAW

1) New Zealand Privacy Law

Privacy law in New Zealand is governed by the Privacy Act 1993 (“the Act”). The purpose of the Act is described in its long title:

“An Act to promote and protect individual privacy in general accordance with the Recommendation of the Council of the Organisation for Economic Co-operation and Development Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, and, in particular,—

(a) To establish certain principles with respect to—

(i) The collection, use, and disclosure, by public and private sector agencies, of information relating to individuals; and

(ii) Access by each individual to information relating to that individual and held by public and private sector agencies; and

(b) To provide for the appointment of a Privacy Commissioner to investigate complaints about interferences with individual privacy; and

(c) To provide for matters incidental thereto.”

The Law Commission issued a report called *Electronic Commerce Part Three: Remaining Issues* in which found that the Act provides a high level of protection for New Zealand consumers dealing with New Zealand based companies. The report stated that:

“The Act is technologically neutral and applies to the electronic commerce sector as well as the paper-based environment. The Act provides sufficient protection to ensure that New Zealand consumers are not dissuaded from dealing with New Zealand businesses engaged in electronic commerce on account of concerns over the privacy of their personal information.”

2) The Privacy Commissioner

The office of the Privacy Commissioner is an independent Crown entity. The online office is at www.privacy.org.nz.

The Privacy Commissioner has a number of roles and functions which include:

- a) Investigating complaints and promoting the understanding and acceptance of the information privacy principles (see below);
- b) Establishment of investigation and enquiries teams;
- c) Issuance of codes of practice, which have the effect of modifying the application of any privacy principles.

3) Privacy Principles

Central to the Privacy Act are the 12 Privacy Principles that are set out in section 6 of the Act. Those principles are:

- a) Principle 1: Purpose of collection of personal information;
An agency may not collect personal information unless the agency collects the information for a lawful purpose connected with a function or activity and the collection of that information is necessary for that purpose.
- b) Principle 2: Source of personal information;
The general rule is that personal information is to be collected directly from the individual concerned.
- c) Principle 3: Collection of information from subject;
Where an agency collects personal information directly from the individual concerned, the agency shall take reasonable steps to ensure that the individual is aware of the fact that the information is being collected, the purpose for which it is being collected, the intended recipients of the information, rights of access to and correction of the personal information.
- d) Principle 4: Manner of collection of personal information;
Any agency shall not collect personal information by unlawful means or by means which are unfair or which unreasonably intrude on the personal affairs of the individual concerned.
- e) Principle 5: Storage and Security of personal information;
An agency that holds personal information shall ensure that the information is protected by such security safeguards as are reasonable in the circumstances against loss and against access by unauthorised persons.
- f) Principle 6: Access to personal information;
When an agency holds personal information in such a way that it can be readily retrieved, the individual concerned shall be entitled to obtain confirmation from the agency of the fact that it holds such personal information and to have access to that information.
- g) Principle 7: Correction of personal information;
Where an agency holds personal information the individual concerned shall be entitled to request correction of the information and to request that there be attached to information a statement of any corrections sought but not made.

- h) Principle 8: Accuracy, etc., of personal information to be checked before use;
An agency that holds personal information is obliged not to use the information unless it has taken reasonable steps to ensure that the information is accurate, up to date, complete, relevant and not misleading.
- i) Principle 9: Agency not to keep personal information for longer than necessary;
An agency that holds personal information may not keep that information for longer than is required for the purposes for which the information may lawfully be used.
- j) Principle 10: Limits on use of personal information;
The general rule is that an agency that holds personal information obtained in connection with one purpose shall not use the information for any other purpose.
- k) Principle 11: Limits on disclosure of personal information;
The general rule is that an agency that holds personal information is not to disclose it to anyone or any body or agency. The exceptions to this rule include authorisation by the individual concerned; necessity for the maintenance or enforcement of law; or the disclosure being one of the purposes for which the information was held in the first place.
- l) Principle 12: Unique identifiers.
An agency shall not assign a unique identifier to an individual unless the assignment of that identifier is necessary to enable the agency to carry out one or more of its functions efficiently.

4) What is “Personal Information”

The Act defines personal information as “*information about an identifiable individual*”.

This definition has been further defined in the case of *Proceedings Commissioner v Commissioner of Police [2000]* in which the Tribunal stated that so that as long as the information “*had the capacity to identify [the individual] to some members of the public*”, it was personal information for the purposes of the Act. The Tribunal went further and said “*in other words, it is not necessary, on this issue of identifiability, that an individual should be able to be identified to the world. It is enough that they are able to be identified by anyone who can make an identification as the result of the receipt of personal information not previously known.*”

5) International Privacy Law Developments

A key characteristic of the Internet is that it is border-less. These days we can sit at home or at work and travel from country to country through cyberspace. This means that protection of privacy on the Internet must be dealt with on an international level.

Key international privacy protection developments are:

- a) The 1980 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. This report sets out principles for

privacy protection which were influential in the development of privacy law in New Zealand, Australia, Canada and Hong Kong.

- b) The 1999 OECD Guidelines for Consumer Protection in the Context of Electronic Commerce. This report focuses on business – consumer transactions and identified the 1980 Guidelines as the appropriate method of achieving effective consumer privacy protection.
- c) The 1981 Council of Europe Convention No 108.
- d) The 1995 EU Data Protection Directive (the Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data). This directive focuses on the limitation on the transfer of personal information out of Europe except to countries that ensure an adequate level of privacy protection.
- e) The 1990 United Nations Guidelines for the Regulation of Computerised Personal Data Files.
- f) The 1998 Federal Trade Commission Report - Privacy Online: A Report to Congress. This report sets out principles for fair information practice that are consistent with consumer privacy interest.

PART II: BIOMETRICS

6) Types of Security Systems

The different types of security systems that businesses may adopt can be categorised as follows:

Type	Indicators
What we know	Passwords, pin numbers, knowledge about us (eg family history)
What we have	Keys, passwords, electronic keys and tags, credit cards, smart cards, chip implants (?)
What we are	Biometrics

7) Types of Biometrics

Type	Usability Status	Information Rating
Fingerprint - optical & electro-optical	Most common method in use. Does not measure whether finger is 'alive'	Medium to Low
Fingerprint - capacitive	The latest technology – measures the natural electrical charge in the skin – can detect between an alive and dead finger. Can also measure blood pressure	Medium to High
Iris Scans	Used now but expensive. Reading requires identification despite biometric distortion through drugs, illness, stress	High
Retinal scans	Not commonly used – said to be less accurate than iris scans	Medium to High

Type	Usability Status	Information Rating
Handprints	In use at US Airports for rapid entry	Medium to Low
Voice prints	Used now but expensive and prone to false negatives. Can detect stress.	Medium
Face scanning (eigenfaces)	Used now. Can generate false positives at low threshold settings by use of face masks as no capacitive measuring. Can detect emotional state	Medium to High
Face scanning (thermo grams)	Not commonly in use but has advantage of prevention of false positives from use of face-masks. May appear in multi-modal devices.	Medium to High in multi-modal environment
Lip movements	Used in experimental multi-modal systems to provide protection against breach through use of face masks etc	Not applicable
DNA	Not practical at this stage as a real time technology but predicted to be practical in some form in the future through saliva test.	Not applicable but if used then VERY HIGH
Multi-modal	Multi-modal systems offer the potential for real time testing of both physical and mental health	VERY HIGH

8) Propositions for Discussion

The following propositions will form a basis for the case study. Attendees will be asked whether they agree with the following propositions:

- a) Employers are entitled to protect their property from loss?
- b) Employers have a duty to employees to protect them from other employees that might be a danger to their personal safety?
- c) Employers are entitled, with the proper consent of the employee, to monitor an employee's health?

9) Scenario 1

Paranoid Corporation, issues an expensive portable to a road warrior analyst, Harriet Geek. The portable will contain very confidential information. The PC is issued with a web cam and fingerprint scanner. Paranoid Corporation requires Harriet Geek to use a fingerprint scanner and retina scanner to access both the portable and the network. This means that the fingerprint and iris scan are registered on both the portable and the corporate network. The portable has, for ease of use and convenience, a pre-configured VPN connection to the corporate network, the logon across the net involves transmission of the 2 biometrics during the insecure phase.

Harriet Geek seeks advice, as she knows that no system is perfect and she is worried about her personal biometrics being stored on the portable, corporate network and transmitted across the net.

- a) What advice can we give to Harriet Geek?

10) Scenario 2

Paranoid Corporation becomes more paranoid.

It realises that the biometric scans contain information about the health of the employees. Is worried about cocaine use in a particular team and personal safety of employees after a nasty incident where a drug affected employee assaulted another.

- a) Should Paranoid as a good employer monitor the biometrics to detect drug crazed employees?
- b) Should Paranoid act if it detects a drug crazed employee?
- c) Should Paranoid's action include automating the physical access security system to exclude the drug-crazed employee?

11) Scenario 3

Paranoid Corporation becomes even more paranoid.

Paranoid Corporation has a very generous health plan. It is a major employee benefit and requires full ongoing disclosure by Paranoid to the HMO to ensure that the HMO is kept informed of sick leave so that it can proactively manage employee health. The plan has won major business awards for its coverage and implementation but is very expensive. Paranoid's CFO, Joe Toecutter, realises from anonymously data mining of the biometric scans, that many employees covered by their health insurance plan are distinctly unhealthy.

Mr Toecutter consults with the HMO and negotiates a 25% reduction in the premiums for Paranoid's health plan on the basis that the biometric data will be fed, in real time, to the HMO. The plans are to enable, for example, the HMO computers to generate real time alarms if an individual employee generates symptoms that would indicate a heart attack is likely. Paranoid's CLO (Chief Legal Officer) has examined the plan and ensured that the biometric data, at the individual level, is kept blind from Paranoid and has advised that the existing employees consent to the HMO and the employment contract covers this plan without requiring amendment.

The executives at Paranoid think this idea is the best thing since sliced bread.

Harriet Geek and her soul buddy in her team, Gatesy Nerd aren't so sure.

- a) Should Paranoid as a good employer allow the HMO to monitor the biometrics of the employees?
- b) Would we change our mind if a trial showed that an ambulance arriving at work as an employee had a massive heart attack, saved the life of that employee who just incidentally, was a solo parent of 11 children?

12) Scenario 4

Note for Scenario 3: The media predictably went crazy over this story and CNN showed interviews of the grateful weeping children on TV endlessly for a week thus permanently altering public opinion. The Privacy Commissioner was lynched outside his house for daring to question the wisdom of this miracle.

Paranoid's Board however did listen to the arguments of the Privacy Commissioner before he was so unceremoniously despatched from this earth, and banned the data link until a legislative framework was implemented.

They did this on external counsel's advice that Paranoid had created a rod for its own back and would be liable for damages if the network failed and an employee was thus not saved.

On stopping the data feed, Paranoid lost the 25% discount. Shareholders have instituted a class action against the Board for failing to save Paranoid the substantial amount of the discount.

To add to the Board's woes, a group of pro-monitoring employees have instituted a class action for endangering their health.

Finally, to add injury to insult, a group of anti-monitoring employees have also issued a class action alleging invasion of privacy.

- a) What do you advise the embattled Board of Paranoid to do (apart from resign or take their own lives)?

13) A Final Word on Biometrics

"We hope that a pervasive, accountable use of biometrics technology will help establish a more open and fair society."

Professor Anil Jain of Michigan SU, Dr Sharath Pankanti and Dr Ruud Bolle of IBM in IEEE Computer, February 2000 at p 48 in their article titled "*Biometrics: The Future of Identification*"

SCHEDULE: BIOMETRICS RESEARCH MATERIALS LIST

Source Type	Material	URL
Journal IEEE - Computer Society edition of 'Computer' February 2000	The edition of Computer was devoted to Biometrics and contains articles titled: <ul style="list-style-type: none"> • Biometrics: The Future of Identification • Face Recognition for Smart Environments • An Introduction to Evaluating Biometric Systems • A Multimodal Biometric Identification System • An Iris Biometric System for Public and Personal Use • Federal Biometric Technology Legislation 	http://computer.org
Consortia/ Standards/ Research	White papers and background material	Biometric Consortium www.biometrics.org FVC2000 http://bias.csr.unibo.it/fvc2000 International Biometric Group www.biometricgroup.com SJSU Biometrics www.engr.sjsu.edu/biometrics
Market Research	Market research market shares published in Dec 2000	http://www.simpletechnology.com/biometrics/smartreseller_2001.pdf
Product Manufacturers	Product information white papers, video tours etc	Iridian – iris scanning system www.iriadtech.com Sony – PC Magazines (US Edition) Best Product Award on fingerprint recognition June 2001 – a capacitive scanner on a USB cable www.sony.co.jp/en/Products/puppy Viisage - Eigenface recognition www.viisage.com Qvoice – multi-modal access control (voice, face, and fingerprint) http://www.qvtrek.com/