Chisholm Health Ethics Bulletin (Autumn 2004) 9(3):4-6
Available at www.chisholm.healthethics.com.au

Privacy, Biometrics, Technology and Health

This is part 2 of a two part series about privacy in health care. Part one discussed general privacy issues and this article examines the impact of technology in regard to privacy and security in health care. As technology becomes 'normal' for everyday living, the idea of privacy as we know it has changed. It is suggested that the idea of privacy is 'a distinctly modern phenomenon and that contemporary understanding about the protection of privacy has evolved not despite new technologies, but because of them'.[1] In the near future biometric technology may become as commonplace as the use of PINs and ATMs are today.

What is biometrics?

The term biometrics is derived from the Greek words *bio* and *metric*, meaning 'life measurement'[2] and is the science that involves the statistical analysis of biological characteristics, and the application of computational methods to biological features, especially with regard to the study of unique biological characteristics of humans.[3] Increasingly, biometrics is associated with identification and authentication technologies used to enhance security. Biometric technology is suggested to have implications for human rights in general, and privacy in particular, as its potential to exploit people or exert social control is unregulated.

Biometric technologies use characteristics such as appearance, (descriptions as used in passports), natural physiography (measurements as in retinal scans), bio-dynamics (as in manner of writing a signature), social behaviour (as in style of speech), and imposed physical characteristics (as in embedded micro-chips), to maintain privacy and security.[4] Traditionally, surveillance of individuals was characterised in terms of who they were or what they were doing, but now technology can track where they are, where they've been or where they are going.[5] Passwords and access codes are commonly used in health care. The ability to remain 'anonymous' is threatened.

Biometric use in securing privacy

Biometrics used for verification asks 'Am I who I say I am?' and works by comparing an individual's previously stored piece of biometric data against an actual physical biometric as read by a scanning device, functioning similarly as a PIN number, password or signature.[6] Such 'one-to-one' searches mean that there is no need to search or match to a central database.[7] Biometrics used for identification, eg forensic comparison of fingerprints from a crime scene against a collection of prints from persons previously convicted of serious criminal offences, asks 'Who am I?' This is a 'one-to-many' match wherein a biometric presented by a person is compared against all biometric samples stored in its database.[8] A match should only be possible if the data is already on file.

The primary objective of most biometric schemes is to heighten security. That is, tracking who is in a particular location at a particular time, who conducted a transaction, or provided data, and the authentication of the identity of those who perform, or seek to perform, a particular act, eg. gaining access to premises or gaining access to data.[9] Unfortunately there is potential for these systems to be abused,

resulting in discrimination or exclusion. Actual collection of a biometric may involve bodily trespass. The system may falsely reject an individual, or wrongly identify them. These schemes may enhance security but at the same time incur some loss of privacy. How does one protect what is private and personal about oneself? Biometric data has a long history in health care but only recently has its use been extended as a means of maintaining security and privacy in health.

Biometric Technology threats to privacy and health

Identity theft is rising as a result of the way technology is used and how criminals exploit it for fraudulent purposes. Biometrics is proposed as a solution to combat these threats, yet they are not foolproof. We all thought passwords and PINs were safe yet we now know that they can be stolen. Passwords and pin numbers can be changed. When criminals find a way to duplicate or 'steal' fingerprints or retinal scans used for biometric security schemes and commit identity fraud, it will be impossible for the victim to change their iris or fingers!

There are reports that organisations face opposition in implementing biometric technologies due to fear that they may pose a health risk, eg. concern that eyes can be damaged by iris scanners. The prospect of continuos monitoring may cause stress for some people. Not all industries need to know who is where and when all the time. Consent is implied in some schemes, but others are 'non-consenting' such as 'facial-recognition' technology proposed to be adopted in Australian airports to help prevent passport fraud, people smuggling and other transnational crimes.[10]

Biometric technology and health

The concern about using human tissue or fluid as a biometric, whilst remote at present, is technologically possible. How the tissue or fluid is processed is not so much a privacy concern, but how it is obtained is, and what eventually happens to 'stored data' or 'samples' is very problematic. Workers may be coerced into enrolling into such schemes fearing their jobs, entitlements, and prospects may be jeopardised if they do not. Unscrupulous employers may use such samples beyond their 'authentication' purposes and screen their employees for genetic diseases and discriminate on the basis of these results. This may seem extreme, yet genetic testing of employees without their knowledge or consent has been reported in the US.[11]

Biometric medical devices are commonly used for therapeutic reasons, not surveillance. These include implanted devices, such as cardiac pacemakers. There was a push to use biometric tracking devices in certain groups of people, eg. those with dementia, and children. Many consider this technology to violate privacy principles. Another point of view is that imposed physiographic identifiers treat a person in a manner similar to inanimate goods on a production line.[12]Others call it a form of restraint. Such technology is available and has been utilised, but with limited support [13]. In some countries newborn babies are being tagged with barcodes that alert security systems if tampered with, in an effort to reduce baby snatching from hospitals.[14] Using implanted medical devices for surveillance purposes is possible, yet is clearly outside their original purpose.

Health Workplace surveillance

There is a tremendous push to computerise many aspects of health care. Many workers in health care now use the computer for much of their day to day work. There

has been ongoing debate about the privacy of workers, in particular, their access to, and use of, e-mail and the Internet, with suggestions that employers have the right to monitor such activity. The World Wide Web has increased the traffic of information. Health workers can post questions about puzzling medical cases to appropriate discussion groups, or browse the net seeking information. Due to certain in-built mechanisms, it is possible to track and record which sites are visited, (through cookies). This information may be sold to direct marketers, without the user's knowledge or consent.[15]

Employees are a vulnerable population in terms of workplace monitoring. The vulnerability of employees in terms of being research participants has been recognised by the NHMRC Human Research Ethics Committee.[16] But most workers are not research participants, yet may be subjected to constant surveillance, which may contribute to stress-related disease. Random drug testing in the workplace is proposed to reduce workplace accidents, though the fear of monitoring is suggested to be a contributing factor in the first place.[17] On the other hand, employers have a duty of care to protect their product as well as their employees. In health care, patients are owed a duty of care to be treated by competent health professionals.

'Function Creep'

How probable is the likelihood that physiological data will be used outside the parameter of health care diagnosis, treatment and research? Once captured, it could be speculated that physiological data about an individual could be used in discriminatory ways. Such issues have been raised about genetic privacy in Australia.[18] The tendency to use something beyond its original intent is sometimes referred to as 'function creep'. There are controversies about the storage of human tissue and fluids obtained for health related purposes. We know that 'data-bases' can be bought and sold. Information from a range of sources can be used to identify someone. It would be a moral and legal outrage if stored data were used to discriminate against or exploit people in some way. Yet the potential to do so persists, and laws can be changed to allow this, despite the moral objections.

For example, a person may say they would never submit to having a genetic test. Yet their potential genetic information may already be stored somewhere, without their knowledge. Indeed the ownership of relinquished specimens has been debated. Another huge repository of potential information about people's individual and family DNA has been captured on Guthrie cards used for newborn screening. The storage and possible use of this data is contentious.[19] Permitting use of human tissue or fluids in the biometric context raises the same ongoing concerns about use beyond the initial imperative, as well as ownership and storage issues.

Saving privacy

The spectre of 'Big Brother' always watching, as fictionalised by George Orwell[20] is becoming fact. Such a society should be anathema, yet aspects of privacy are eroded away without debate or discussion. Video or closed circuit TV surveillance is commonplace. Use of PIN numbers, access codes, individual swipe cards, passwords, Tax File Numbers, etc can be monitored. Mobile phones can be used as tracking devices. The list is long. The health care industry is looking towards technology to maintain privacy and security. Biometric technology used in non-therapeutic ways, such as for security, may violate aspects of our right to be left alone. The *Biometrics*

Institute has begun public consultations on a proposed 'Privacy Code of Conduct' for the biometrics industry in Australia, which is currently unregulated.[21]

Can we, or should we turn back the clock? Is it imperative that we give something up, such as some privacy, to get something we desire, such as increased security? How secure is all this information about us? Technology has made a mockery of the word privacy, as more technology is rolled out to ensure our security in using technology in the first place. So we give away a fingerprint, a snippet of DNA, a certain way we walk. We allow this information to be stored in huge databanks on our behalf and for our benefit, to prove that we are who we claim to be. It is ironic how we engender such conditions of paranoia about protecting our privacy, that we feel compelled to expose more about ourselves to satisfy the conditions of maintaining our privacy in the first place.

Endnotes

[1] R Salecl The exposure of privacy in today's culture. (Part 1: Public/Private The Distinction), *Social Research*, Spring, (2002) 69(1):9
[2] Biometrics Australia, http://www.biometricsaustralia.com/index.html accessed 7/11/03.
[3] R Hopkins, An introduction to biometrics and large scale civilian identification, *International Review of Law, Computers & Technology*, (1999)13(3):337-363.
[4] R Clarke, Biometrics and Privacy, http://www.anu.edu.au/people/Roger.Clarke/DV/Biometrics.html, accessed 18/8/03.
[5] Carson Analytics *Privacy Guide*, http://www.caslon.com.au/privacyguide19.htm, accessed 26/11/03.
[6] Richard Hopkins, 1999…
[7] A Cavoukian, Information and Privacy Commissioner of Ontario, Canada, cited by Biometrics Institute, *Biometrics Privacy Code Discussion Paper*, http://www.biometricsinstitute.org accessed 12/9/03, p. 9
[8] R Hopkins, 1999…: and Roger Clarke…: and A Cavoukian, p. 9.
[9] R Clarke …
[10] 'Living Proof', *E-Bulletin* April 30, 2003, http://bulletin.ninemsn.com.au/bulletin accessed 19/12/03 : and 'Australia could be first to use biometric passports', *The Age*, 5 June, 2003, http://www/theage.com.au/articles/2003/06/05/1054700309896.html accessed 7/11/03.
[11] M Friedrich, Preserving Privacy, Preventing discrimination becomes the province of genetics experts, JAMA, (2002) 288(7):815-819.
[12] R Clarke, 1994, *Human Identification in Information Systems: Management Challenges and Public Policy Issues*, http://www.anu.edu.au/people/Roger.Clarke/DV/HumanID.html accessed 12/11/03.
[13] D Appell, Getting under your skin, *Scientific American*, (Jan 2003) 288(1):18.
[14] BBC News, 22 Jan 2003, 'Barcodes 'stop baby mix-ups', http://news.bbc.co.uk/1/hi/health/2680249.stm accessed 12/11/03.
[15] R Sikorski, R Peters, 'A privacy primer for the web: Spam, bread crumbs, and cookies, *JAMA*, (1998) 270(15):1219-1220; and M O'Reilly, 'Your secrets aren't sacred', *CMAJ-JAMC*, (1999) 160(13):1859.
[16] NHMRC, *Human Research Ethics Handbook*, Commonwealth of Australia, 2002, p. C.60.
[17] P Holland and M Wickham, 'Drug testing in the workplace: unravelling the issues', *Journal of Occupational Health and Safety – Aust NZ*, (2002) 18(1):55-59.
[18] Australian Law Reform Commission, *ALRC 96 Essentially Yours: The Protection of Human Genetic Information in Australia* as at 13 March 2003, http://www.austlii.edu.au/au/other/alrc/publications/reports/96/ accessed 29/10/03.
[19] Victorian Privacy Commissioner, 'Securing the collection of 2 million Victorians' DNA', *Privacy Aware*, (2003) 2(2):3
[20] George Orwell, *Nineteen eighty four*, Penguin, (London: 1989)
[21] Biometrics Institute Media Alert, *Biometrics Institute invites community input on new privacy code of conduct for biometrics*, Wednesday, 10 September, http://www.biometricsinstitute.org accessed 12/9/03.