The Impact of Legal and Social Issues on the Acceptance of Biometrics

Stuart Irvine - Researcher
Rodger Jamieson - Director

SEAR: Security, E-Business, Assurance Research Group
School of Information Systems Technology and Management
University of New South Wales
e-mail: r.jamieson@unsw.edu.au

Abstract

This paper presents initial research into investigating the viability of large-scale biometric technology implementations. Literature provides considerable support to technical aspects of biometric viability, but there appears to be limited research concerning the equally significant hurdles facing social acceptance. It is argued that any large-scale social acceptance of biometrics will need to be achieved through a combination of legal and architectural control mechanisms established to allay social fears concerning the opportunities for the abuse of biometric systems. This paper considers a cross-section of legal concerns and controls before outlining research questions to be examined and a methodology for a discovery of issues and viable control mechanisms.

Keywords

Biometrics; Legal; Social; Identification; Authentication; Privacy

INTRODUCTION

Electronic crime is increasingly an area of concern to governments, organisations and individuals. In an existence significantly reliant upon computers and the Internet for day-to-day tasks (ranging from general communications to financial transactions) the scope for criminal exploitation of electronic resources is already significant and continuing to expand. The 2002 Australian Computer Crime and Security survey, for example, found that between 1999 and 2002 the number of computer crime and security incidents doubled, and the 2003 survey placed total losses of computer crime at more than double that of 2002. One area currently under high scrutiny is that of identity fraud, both as a crime in its own right, and as a facilitator of other crime. A crucial step in curbing the threat of identity fraud is the introduction of more secure means of verifying identity and/or authenticity; The 2002 Australian Computer Crime and Security survey indicates that it is inadequate customer identification and validation processes which make it easy to defraud on-line merchants.

Traditional means of authentication and identification and their weaknesses are outlined before providing a more in depth discussion of biometrics and arguments that have been raised for and against their use. As an example of inhibitors to the large-scale acceptance of biometric technology in everyday life, several acceptance issues are then raised.

The aim of this research is to provide a starting point for research that will look to discover the main inhibitors to biometric acceptance, and what controls are required in order to overcome these inhibitors. The paper concludes with discussion of a proposed research methodology for such discovery.

An appropriate starting point for discussion on validation technologies and issues is the concepts of identification and authentication. Although often used synonymously, there are important distinctions between these concepts. Identification entails the matching of certain criteria to civil identity, for example the matching of a fingerprint found at a crime scene to a fingerprint stored on a police database (Tomko, 1998). In contrast authentication needs no inherent reference to an 'identity'. Authentication is a process of examining the characteristics of an individual to verify their eligibility to access a particular service and need not necessarily hinge on identification (Clarke 2002). For example, knowing that the person to whom you are selling alcohol is over 18 is imperative, but identifying the individual as Jane Smith, at x address etc is irrelevant. It should be noted here that the law dictates that some transactions do require identification. For example, the Australian Commonwealth Electronic Transactions Act 1999 dictates that in any transaction requiring a signature a method must be used to identify the person in question. (Electronic Transactions Act 1999 (Cth), Sect 10(1)(a)).

Techniques for identification and authentication have often been explained in terms of three categories (Kim, 1995, p. 206; Campbell et al., 2003, p. 39): testing what a person knows (eg a password); testing what a person possesses (eg a token); and testing who a person is (eg a fingerprint). Some verification schemes, referred to as multifactor methods, rely upon a combination of at least two techniques, the most common example perhaps that of access to a banking Automatic Teller Machine – requiring both something to be possessed (a bank card) and something to be known (the pin number associated with that particular card). Such validation schemes provide a significantly higher level of confidence than the use of single factor schemes, but can still be relatively easily compromised given sufficient motive and resources (Ashbourne, 1999, p. 1).

The major problem with the first two of these schemes, what a person knows or possesses, is that knowledge or possession is simply that. Although a security system using these techniques dictates this be interpreted as an authorised individual, it is not the individual who is identified – it is the object or knowledge, easily divorced from the actual person holding it (Ashbourne, 1999).

> *"...A major problem with current authentication technology is that there is no way to positively link the usage of a system to the actual user. ... Remote authentication policies based on a simple combination of user id and password, or, worse, simply based on possession, have become inadequate" (Bolle et al., 2002, p. 2727).*

The increasing desire for users to be able to access systems and resources remotely, and the need for such access to be both secure and non-repudiable, points towards the need for stronger methods of verification. Biometrics have long been considered for the next step in the evolution of validation techniques. MasterCard for exampole claims that the addition of smart-card based biometric authentication at point of sale credit card payment will reduce fraud by 80% (Liu and Silverman, 2001). Issues relating to both technical development and societal acceptance of biometric systems, however, have the potential to plague practical implementation.

BIOMETRICS

The term biometrics, strictly speaking, refers to "the statistical analysis of biological phenomena and measurements" (Kim, 1995, p. 206). Its use in relation to authentication and identification has come to also include the actual technologies behind the implementation of such systems (Kim, 1995, p. 206). Biometrics falls into the third category of validation techniques – who a person is; validation via unique physiological and/or behavioural characteristics. The most common physical characteristics used include fingerprint patterns, iris patterns, retinal patterns, facial recognition and hand geometry, whilst characteristics such as voice and handwriting fall under the category of behavioural biometrics.

Biometric acceptance issues

Biometrics have come under increased consideration for use in validation scenarios due to the advantages offered over more traditional methods. Unlike the 'what a person knows' or 'what a person has' approaches to identification, biometrics are (with very few exceptions) unique and cannot be "*forgotten, forged, duplicated, misplaced, or stolen*" (Campbell et al., 2003, p. 32).

The technical feasibility of biometric systems has been the subject of much research and is beyond the scope of this paper. Technology, it would seem, is now at the point of offering relatively stable biometric systems but running parallel to technological concerns are issues relating to the general acceptance of biometric systems. Concerns regarding the use of biometrics include factors such as the invasiveness of the procedure, potential hygiene issues, the association of biometrics with criminality, and issues relating to the protection of personal privacy.

Privacy Concerns

Perhaps one of the largest barriers to a full-scale acceptance of biometric technology can be found in issues relating to privacy, so much so that one author claims the widespread integration of biometrics into society as a verification tool is no longer "an engineering challenge, [but] a marketing challenge" (Douglas, 2002). The long-standing argument between those who seek security and are willing to trade certain amounts of individual privacy to achieve this, and hard-line civil libertarians who see any trade off as an irreversible slide to an Orwellian society of surveillance has found a new battleground in biometrics.

One of the key features of biometrics under argument, in both the for and against camps, is the claim that biometrics have the ability to unquestionably tie an individual to his or her chosen identity; that they can be used as universal identifiers having the potential to link or associate any number of sources of personal information to an individual, either with or without consent (Tomko, 1998).

There are many people who argue that the potential for the misuse of biometrics as a strong identifier is far too high, and the consequences of such misuse too dangerous to society. U.S. representative Frank Horton, speaking on a proposed national data centre in America, stated:

> *"One of the most practical of our present safeguards of privacy is the fragmented nature of present information. It is scattered in little bits and pieces across the geography and years of our life. Retrieval is impractical and often impossible. A central data bank removes completely this safeguard" (In Clarke, 1987, p. 5).*

Clarke (1987) argues that centralised storage is no longer a pre-requisite to the eventuation of such a dossier society, which can be achieved with the existence of three conditions: A range of personal data systems; telecommunications interconnection between data systems; and a consistent identifier between the data. The first two conditions are already satisfied in current technology, and biometrics would appear to be a prime candidate to fulfil the third.

The principal concern is that an identifier that is both universal and unique provides the potential to very easily create 'information trails' on individuals (especially taken in tandem with an increasingly online world): that "*a biometric such as a fingerprint ... can be used to trace peoples transactions and link massive amounts of personal data about them*" (Tomko, 1998); "*[They] create the potential for personal information from different sources to be linked together to from a detailed personal profile about that individual unbeknownst to him or her. This represents a clear invasion of privacy; one to which most people would object.*" (http://www.findebiometrics.com/pages/privacy.html) The feared logical conclusion of data on individuals being collected en-mass is that personal privacy becomes compromised to the point of non-existence. Clarke (2001) paints a particularly bleak Orwellian picture of dehumanisation as the ultimate conclusion of biometrics:

> *"Authoritarian governments ride rough-shod over personal freedoms and human rights. They will establish legal authority for and enforcement of the capture of biometrics for every transaction, and at every doorway. Such governments see consent and even awareness by the person as being irrelevant, because they consider that the interests of society or 'the state' dominate the interests of individuals."*

Another concern relating to biometrics is the claim of non-repudiability, and whether in any technological implementation such a claim can be defended. The argument advanced is that if society invests 100% faith in biometric identification methods and such methods are compromised (by biometric forgery or some other weakness in the biometric security system), the citizen or consumer is left without recourse.

Technology has advanced at a staggering rate over the past few decades, and there are numerable things once considered 'impossible' but are now relied upon every day. Given this trend, convincing society as a whole that biometrics are completely secure from any form of fraud, forgery, duress or other potential avenues of compromise will be an all but impossible task, and without that conviction the above fears will always exist. If technology cannot guarantee infallibility, the burden of providing a palatable environment for the use of biometrics will most likely fall to a combination of architectural implementation and legal controls ensuring avenues are in place to provide recourse and defence to the citizen or consumer.

Ancillary to this the law may demand alternate forms of verification to be available. If this is the case, then perfect implementation of biometrics or otherwise, the alternate form of verification will be subject to the traditional weaknesses of non-biometric schemes.

MAKING BIOMETRICS VIABLE

Despite all fears and concerns raised against biometrics, the reality would appear to be that the practical benefits offered are resulting in more and more widespread implementation. This being the case the direction of pressure shifts from fighting against the use of biometrics period to considerations of how they are implemented, what they are used for, and the regulation of them. Broadly speaking, in order for biometrics to be broadly acceptable they must be legally and physically robust, safe to use, not invasive of the user's privacy and not perceived as socially unpalatable (Kim, 1995, p. 210).

Considering Lessig's model (1999, p. 86) (Figure 1) of forces that regulate and control, the two primary areas acting directly on Biometrics could be argued to be architecture and law. Social and market forces will influence biometric implementations, though it may be argued that this influence will be indirect, acting through the other controlling factors. Architectural solutions concentrate primarily on implementation – achieving regulation by building into the system what is and is not physically possible to achieve. Legal avenues approach from a different angle, dictating what is and isn't permissible through legislation and threat of penalty. Biometric regulation will most likely be found in a combination of the two forces. Even if architectural solutions reach the point of allaying all social fears by making it impossible to compromise systems and invade personal privacy a problem still exists. It may be argued that the governments will not allow a 'perfect' solution, requiring a 'back door' of some description be built in to the system so under certain circumstances control mechanisms protecting privacy can be pushed aside. (Refer Figure 2).

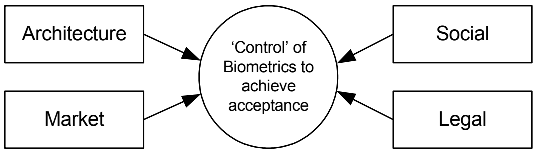

Figure 1: Lessig's model of forces that regulate.

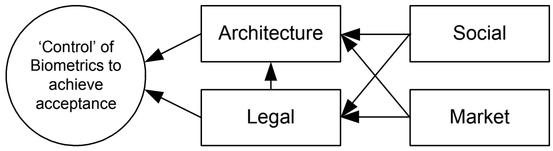

Figure 2: Model of Forces directly controlling biometrics

An example of such a trade off occurring is seen in the use and implementation of encryption technology. Architecturally (as far as is known) there is nothing stopping individuals creating purportedly unbreakable codes (consider arbitrarily large keys implemented with public/private key cryptography). Governments, however, have proven to be wary of such a possibility, attempting to curb this situation via law with systems such as key escrow, and straight out banning of the use of certain forms of encryption.

Legal 'Regulation'

In conjunction with architectural regulation (see for example Tomko, 1998 and Bolle et al 2002) more and more consideration is being given to what legal issues must be addressed, either by developing an appropriate legal framework, or, at the least, in interpreting extant legal controls in a new scenario.

While there are numerous legal issues surrounding biometrics, this paper will focus on the broad category of privacy issues relating to the widespread uptake of biometrics in society, which comprise primarily concerns of surveillance and personal data protection (Kim, 1995, p. 212). Other issues not discussed include issues and concerns of fundamental human rights (Prins, 1998, p. 161); the use of biometrics as legally admissible evidence (Prins, 1998, p. 163); in the scenario of non-voluntary acquisition of biometrics (generally by a government agency) whether the taking of biometric measurements constitutes a search and whether such a search is reasonable (Nuger).

It is worth mentioning briefly the issue of discrimination against minorities in relation to the implementation of biometrics (Dunstone, 2001, p 7). In order to achieve a completely non-discriminatory use of biometric technology, it must be guaranteed that no user group or individual is excluded – either in civil or private applications. Such exclusion could stem from either physical or social concerns; for example, in some cultures looking a person in the eye may be deemed socially unacceptable, which would preclude the use of retinal or iris scanners (Prins, 1998, p. 161). For such a guarantee to be realistically achieved, substitute procedures for authentication or identification must be provided, and if this is the case then the security hoped to be achieved via the implementation of biometrics is potentially denigrated to the lowest common denominator of non-biometric systems regardless of the infallibility of biometrics themselves (Albrecht, 2001, 7).

Personal data protection

Privacy, it has been said, is not so much about complete secrecy, but about the control of personal information. Most people realise that complete secrecy and privacy are, aside from all utopian ethical arguments and concerns, a practical impossibility. Under that reality, concerns shift from a fear that organisations or governments possess and gather personal information to a fear of why it is gathered, along with what is or can be done with it. Such concerns have been growing for some time now, such that many governments have put in place specific legislation attempting to prevent the potential misuse of personal information. International conventions have also developed a set of guiding principles, stating for example that data should not be used for purposes other than the original purpose of collection without either the authority of law or the consent of the individual (Kim, 1995, p., 213).

The Australian constitution offers no enshrined right to privacy, resulting in such a right being dealt with under a patchwork of individual Commonwealth and State/Territory legislation and guidelines. The National Privacy Principles, introduced into the commonwealth Privacy Act (1988) in 1998 for the public sector and 2000 for the parts of the private sector are an example of such legislation, Though have been consistently criticised for their functional impotency (for example Clarke 2002; http://www.caslon.com.au). The legislation sets down 11 'National Privacy Principles', dealing with the collection, use and dissemination of personal data. The act covers personal information, defined as and information or opinion that can identify a person, as well as 'sensitive' information for which it provides special protection.

Application of the national privacy principles to biometrics raises some interesting questions. Principle 1 dictates that personal information only be collected for a purpose that is directly related to a function or activity of the collector, and that the collection of the information is necessary for that function. Principle 3, in turn, states that the information collection must not intrude to an unreasonable extent upon the personal affairs of the individual concerned. While principle 1 would appear to vindicate the collection of biometric data on the argument that it is necessary to the security of the business, principle 3 may qualify this. An argument similar to that used in arguing against biometrics on a human rights basis may be raised, claiming that the taking of a biometric is un-necessarily invasive in situations where other options for identification or authentication exist. (Prins, 1998, p.161) If such an argument is accepted, then again society is left with the requirement of providing alternate means of verification, subject to the threats outlined above.

The clause 'necessary for that function' also has the potentially detrimental effect of providing potential loopholes within the legislation. The US Privacy act has shown to be at best a weak protector of personal data due to a similar clause providing for an exception permitting the 'routine' use of data. In the US scenario, the clause (similar in nature to Australia's 'necessary for that function') was applied so widely that it undermined the effectiveness of the act essentially legitimising almost any dissemination of personal information between federal agencies (Kim, 1995. p. 213; Clarke, 1987)

National Privacy Principle 4 states that any record containing personal information must be:

> *"Protected, by such security safeguards as it is reasonable in the circumstances to take, against loss, against unauthorised access, use, modification or disclosure, and against other misuse" (Privacy Amendment (Private Sector) Act 2000).*

A question arises as to what constitutes 'reasonable' actions. In the case of biometrics, one could argue that the 'circumstances' –the fact that biometrics provide such a strong unique and universal identifier – would dictate that 'reasonable' is a very high threshold, greater than that required of other personal information.

The architectural innovations working in synch with such concerns of personal data privacy are biometric implementations which do not require a central storage of the data. Smart cards, where the biometric template is stored upon, and verified by, a card that never leaves the user is one example (Vanderhoof, 2003, Bovelander and van Renesse, 1995). The problem of data collection, however, still exists and falls under the ambit of the national privacy principles if the usage of the smart card – for example in gaining physical access to a building or logical access to a bank account – is recorded and related back to an identifiable individual. In such circumstances removing the storage of the actual biometric template from the central database does not address privacy concerns.

Right of Procedural Fairness

Another important area requiring legal consideration is that of the right of appeal of an individual who has in some way been disadvantaged on the basis of biometric identification. For example, the New York State Social Services law was amended in 1992 to provide that automated finger imaging may be a pre-condition for enrolment in social welfare programs. The rationale behind such legislation is clearly and inoffensively an attempt to prevent 'double dipping' of welfare benefits. The section also, however, provides for protection of any applicant suspected of fraudulent behaviour by providing that for an individual suspected (on basis of their biometric scan) of multiple enrolments, welfare benefits may not be denied until tried and convicted. (Prins, 1998, p. 160)

The need for such protection should be apparent in any scenario where biometric identification is the sole or even major justification behind an individual being the subject of any serious effect (such as the denial of services, the issues of search warrants etc). Such a policy is consistent with Australia's National Privacy Principle's 6, 7 and 8, providing together the right of an individual to access their own records as well as the obligation upon the body holding the records to take all reasonable steps in ensuring the information is up to date and accurate.

RESEARCH APPROACH

There are several pertinent questions requiring close examination before society will be comfortable with the large-scale use of Biometric technologies. These can be broken down into the following:

- What are the issues that need to be addressed (partially canvassed by this paper)?
- Why are these issues?
- What is the relative seriousness and importance of each issue?
- How will these issues be best dealt with and what measures and mechanisms can be put into place in order to allay fears?

The research methods proposed to address these research questions are primarily qualitative, including questionnaires and semi-structured interviews of legal professionals, IT professionals and both current and potential users of biometric systems. It is envisaged that from these three groups issues and controls will be categorised according to the model proposed above, into considerations directly affecting biometrics and those acting indirectly. Analysis of the data using NVIVO should provide a comprehensive list of issues along with potential control mechanisms, both legal and social, for those issues.

Data analysis will be conducted according to the methodology of Grounded Theory, a process of organising data obtained from the questionnaires and interviews into concepts and themes in order to help understand it. (Blaikie 2000) Grounded Theory is often used as a means of dealing with rich descriptive data without losing contextual complexity (Orlikowski 1993). This is achieved with an interpretivist perspective, drawing from 'a network of assumptions and inter-subjectively shared meanings' (Backhouse et al 2001, citing Burrell and Morgan 1979) as a means of drawing from perceptions and retaining detail while simultaneously grounding the account in the raw data (Myers 2001).

CONCLUSION

While biometric validation techniques do offer much for security in an online world, their future, subject to the privacy versus security debate (already seen in technologies such as encryption), rests in the eventual compromise of two ideals: that under no circumstances should personal privacy ever be compromised, or, that under special situations, such compromise is acceptable. Governments have been historically reluctant to completely forgo the right to monitor private dealings (consider search warrants and wire tapping regulations), and in the current political climate, coloured by events such as September 11, there is no real reason to see this changing. If this is the case, governments will need to ensure that suitable legal and technology frameworks are in place to provide the public with faith that such a potentially oppressive tool is not abused to the point of eradicating the civil liberty of privacy.

REFERENCES

2002 Australian Computer Crime and Security Survey, AusCert.

2003 Australian Computer Crime and Security Survey, AusCert.

Albrecht, A (2001) 'Understanding the Issues Behind User Acceptance.' Biometric Technology Today, January, pp 7-8.

Ashbourne, J (2003) The Biometric White Paper. 1999. [Online]: http://www.homepage.ntlworld.com/avanti/whitepaper.htm [28 May 2003].

Ashbourne, J (1999) Using Biometrics 1999. [Online]: http://homepage.ntlworld.com/avanti/using.htm [28 May 2003].

Backhouse, J. and Dhillon, G. Current Direction in IS Security Research: Towards Socio-Organisational Perspectives. Information Systems Journal, 2001(11), 127-153.

Biocentric Solutions Website. [Online]: http://www.biocentricsolutions.com/faq.html#authentication [28 May 2003].

Blaikie, N. Designing Social Research. Oxford: Polity Press, Blackwell Publishers Ltd Oxford, 2000.

Bolle, Ruud M, Connell, J and Ratha, N (2002) 'Biometric Perils and Patches.' Pattern Recognition, 35, pp 2727 – 2738.

Bovelander, E and van Renesse, R (1995) 'Smartcards and Biometrics: An Overview', Computer Fraud and Security, December, pp 8 – 12.

Campbell, Paul, Calvert, Ben and Boswell, Steven. Security+ Guide to Network Security Fundamentals. Thomson Course Technology, Canada 2003.

Caslon Analytics Privacy Guide. [Online]: http://www.caslon.com.au/privacyguide.htm [28 May 2003].

Clarke, Roger. Information Technology and Dataveillance. 1987. [Online]: http://www.anu.edu.au/people/RogerClarke/DV/CACM88.html [28 May 2003].

Clarke, Roger. The Mythology of Consumer Identity Authentication. 2002. [Online]: http://www.anu.edu.au/people/Roger.Clarke/DV/AnonDPPC02.html [28 May 2003].

Davis, Ann. 'The Body as Password'. Wired, Issue 5.07, July 1997. [Online]: http://www.wired.com/wired/archive/5.07/biometrics_pr.html [28 May 2003].

Derakhshani, Reza, Stephanie Schuckers, Larry Hornak, Lawrence O'Gorman. 'Determination of vitality from a Non-Invasive Biomedical Measurement for use in Fingerprint Scanners.' Pattern Recognition 36 (2003), 383-396. Elsevier Science, 2002.

Douglas, Jeanne-Vida. Biometrics Players to Placate "Gullible Wide-eyed" Public. 2002. [Online]: http://www.zdnet.com.au/newstech/security/story/0,2000048600,20268667,00.htm [28 May 2003].

Dunstone, Dr Ted. 'Getting to Grips with Public Policy.' Biometric Technology Today, October 2001, 7-8. Elsevier Science, 2001.

'Forging Ahead.' Biometric Technology Today, October 2001. Elsevier Science, 2001.

Kim, Hyun-Jung. 'Biometrics, is it a Viable Proposition for Identity Authentication and Access Control?' Computers and Security, 14 (1995) 205-214. Elsevier Science, 1995.

Lessig, Lawrence. Code and Other Laws of Cyberspace. Basic Books, New York, 1999.

Liu, Simon and Silverman, Mark. A Practical Guide to Biometric Security Technology. 2001. [Online]: http://computer.org/itpro/homepage/jan_Feb01/security3.htm [28 May 2003].

Nuger, Dr Kenneth P. Biometric Applications: Legal and Societal Considerations. [Online]: http://www.engr.sjsu.edu/biometrics/publications_consideration.html [28 May 2003].

Orlikowski, W. 'CASE Tools as Organisational Change: Investing Incremental and Radical Changes in Systems Development.' Management Information Systems Quarterly, 17(3) 1993.

Prins, Corien. 'Biometric Technology Law: Making our Body Identify For Us: Legal Implications of Biometric Technologies.' Computer Law and Security Report, Vol 14, no 3 1998, 159-165. Elsevier Science Ltd, 1998.

Privacy, Friend or Foe? [Online]. Available: http://www.findbiometrics.com/Pages/privacy.html [28 May 2003].

Soutar, Colin. 'Implementation of Biometric Systems – Security and Privacy Considerations.' Information security Technical Report, Vol 7, No 4 (2002) 49-55. Elsevier Science 2002.

Tomoko, Dr George. Biometrics as Privacy-Enhancing Technology: Friend or Foe of Privacy? 1998. [Online]: http://www.dss.state.ct.us/digital/tomko.htm [28 May 2003].

Vanderhoof, Randy. 'Smart Cards, Biometrics and Privacy.' Card Technology Today, February 2003, 10 – 12. Elsevier Science, 2003.

COPYRIGHT