Edith Cowan University
Research Online

Australian Information Security Management Conference

Security Research Institute Conferences

2006

Cyber crime and biometric authentication – the problem of

Michael G. Crowley
Edith Cowan University

Originally published in the Proceedings of 4th Australian Information Security Management Conference, Edith Cowan University, Perth, Western Australia, 5th December, 2006
This Conference Proceeding is posted at Research Online.
http://ro.ecu.edu.au/ism/74

Cyber crime and biometric authentication – the problem of privacy versus protection of business assets.

Michael G Crowley
School of Law and Justice
Edith Cowan University
Perth, Australia
Email: m.crowley@ecu.edu.au

Abstract

Cyber crime is now a well recognised international problem that is a major issue for anyone who runs, manages, owns, uses or accesses computer systems linked to the world-wide web. Computer systems are business assets. Personal biometric information is also an asset. Studies have shown that privacy concerns represent a key hurdle to the successful introduction of biometric authentication. In addition, terrorist activity and the resultant legislation have added an additional risk factor businesses need to take into account if they propose using biometric authentication technology. This paper explores the use of biometric authentication to protect business and individual assets. The focus is on protecting the privacy of those who legally access computer network systems. The paper argues that an appropriate balance needs to be established between adequate security and individual privacy.

Keywords
Biometric authentication, privacy, cyber crime, protection of business assets, security.

INTRODUCTION

Cyber crime is a recognised international problem. The problem grows with increasing reliance upon computer network systems for managing of financial, security and infrastructure services. Problems include, hacking, viruses, data theft, fraud, sabotage, denial of service attacks and the associated recognition that terrorists also utilise computer network systems. Computer systems are an integral asset of business practice and smart business enterprises protect their assets. One way of protecting assets is limiting computer system access to identifiable users who use biometric identifiers. Personal biometric access data is also a key business asset. Likewise, individuals who use biometric features to access computer systems should also treat their personal identifying features as a key asset. Identity should be non transferable, because, identify fraud alone is reported as costing consumers and businesses in the United States of America some US$52.6 billion in 2004 while others suggest a lower figure of US$8 billion by 2005, growing at a rate of 30% per annum . It is also a growing problem in Australia. The Australian Institute of Criminology estimates the cost in Australia at between $2 to $6 billion in 2002-3. Studies have also found 13% of New South Wales birth certificates and 18% of Victoria's birth certificates did not match the records of the issuing agency . While cyber crime can be broken down into computer based crime and computer system crime , this paper is concerned with the implications of the use of computer technology to identify individuals.

Terrorists also use computer technology to access information, communicate and distribute propaganda. The rush of anti-terrorism legislation since September 11, 2001 impacts directly upon business, especially the legislation concerned with monitoring cash transactions and identity checks of individuals. Businesses who seek to incorporate enhanced access systems such as biometric authentication need to be aware that biometric technology has business risks that go beyond enhanced security and privacy implications to changing their traditional business-client relationship as a result of their potential involvement in the 'war on terror'. Governments also link terrorists to criminals and have passed new laws promoting universal surveillance of Australian citizens with the result that businesses have a de-facto deputy sheriff role because of the *Financial Transactions Reports Act* 1988 (Cwlth).

In 2001 the Australian Government passed the *Cybercrime Act* 2001 (Cwlth). This legislation is concerned with computer offences and law enforcement powers related to electronically stored data. Significantly, s.201A of Schedule 2 of this legislation makes it an offence for a person with knowledge of a computer system not to assist authorities access a computer system. The legislation also protects staff members or agents of Australian Security Intelligence Service (ASIS) or Defence Services Directorate (DSD) of any civil or criminal liability arising out of a 'computer-related act, event, circumstance or result' (s.476.5 (3) Cybercrime Act), so long as the Inspector-General of Intelligence and Security has given a certificate which will be prima facie proof of the facts certified (s.476.5 (2B) Cybercrime Act). Businesses operating within Australia need to take heed of these legislative changes as they provide authorities, especially when combined with other anti-terrorism laws, significantly increased powers when balanced against the traditional use of search warrants. The scope for governmental agency access to business information database is enhanced while the ability to challenge government action in the courts is reduced.

WHAT IS PRIVACY?

While proper user identification/authentication is crucial for an effective computer network system security, not all computer network systems require the enhanced security associated with biometric authentication. Businesses need to decide whether or not biometric technology is really worth the trouble. Security and privacy are not the same. As security measures are enhanced, the privacy of those who are subject to the enhanced security diminishes. Privacy is at its most basic an individual, personally private concept. There are the classics; 'the right to be let alone' , or 'an Englishman's home is his castle' and, 'the state has no business in the bedrooms of the nation' . Citizens can still maintain this level of privacy so long as they avoid computers linked to the internet, travel, telephones, mobile phones, credit cards, financial institutions and buying certain materials and substances. For the rest there is a trade off between what we want to maintain 'private' and what we will have to give up if we are to actively participate in today's modern world. The new privacy problem for the greater majority of honest, law-abiding citizens is the introduction of surveillance and monitoring systems supported by laws some of which lack traditional legal protections.

MISUSE OF GOVERNMENT POWER AND TECHNOLOGY.

The cry, 'if you have done nothing wrong then you have nothing to worry about' is the cry of the gullible fool who has paid scant regard to history and abuses of populations by governments through the use of technology. In Australia citizens need look back no further than the halcyon days of the State police special branches and the abuses that flowed from unsupervised abuse of the privacy rights of law abiding citizens for what in the end was politically motivated intelligence gathering, not supposed protection of the community . Some decades ago in Argentina, for example, citizens carried national identity cards with a photograph on the front and a complete set of fingerprints on the back . The information was stored centrally on a system known as Digicom. By combining digital processing with radio technology police, who have stopped citizens, scanned in fingerprints and relayed the information from police cars back to the central database. Between 1976 and 1981 some thirty thousand Argentine citizens disappeared, facilitated by technology . Not so long ago the Chinese Government made arrangements with Goggle and other internet providers to monitor Chinese citizens on the internet. Political dissent is not tolerated in mainland China.

Could this happen in Australia? For now, September 2006, this is unlikely; but times are changing. The new anti-terrorism laws combined with the Howard Government's expedient statements on the children overboard from the Tampa incident on the eve of the 2004 Federal Election and the putative presence of Weapons of Mass Destruction in Iraq to justify Australian support of the American invasion, rather than an emphasis on the truth, shifts the balance towards potential government control of information, and hence its citizens. Information provides a means of control. For example, what have you done, read, said, written that if made public would cause you to feel uneasy, worse embarrassed, might affect future employment or make you a target of politically motivated interest groups as happened in the 1950s with McCarthyism in the United States of America?

In Australia governments have failed with attempts to introduce an Australia Card. However, the tax file number is rapidly becoming the default unique identifier of Australians. In the United States of America the Social Security Number became a de-facto unique identifier with social security number fraud widespread. The stricter requirements of proof needed by citizens who seek to open bank accounts, obtain licences and passports means a lot more institutions/businesses hold key identification data on an individual citizen. Computer network systems have the capacity to link these separate institutions/businesses together. Biometric authentication will allow a higher degree of certainty that citizen x was the same person who carried out a series of financial transactions, moved from point a to b to c, purchased products by credit card and used specific computer networks to look at identifiable information.

While only time will tell whether or not such systems in Australia become an Orwellian reality , recent news from the United States illustrates the privacy problems individuals face if they use the internet. Google users ask Google questions and access Google's databases. Google stores this information, the information about who asked for what. Recently 23 million searches made by 650,000 customers over a three month period were unexpectedly made available and what made this important was that the use of numbers to hide the individual identification of Google users did not work . One of the means of identification was by looking at what was searched and then looking at where the 'searcher' accessed the internet for the search.

Australian legislation such as *Privacy Act 1988* (Cwlth) and the *Privacy (Private Sector Amendment) Act 2000* (Cwlth) protects personal details taken by organisations and institutions in the course of business. While this legislation would also protect the personal details taken in the course of setting up a biometric system, it is of no use in the above Google incident. There is also no effective legislation to protect individual biometric data. Present privacy legislation does not contemplate biometric authentication/identification. Furthermore, identity security was considered a 'key concern' of the Council of Australian Governments' Communique which also agreed to 'investigate the means by which reliable, consistent and nationally interoperable biometric security measures could be adopted by all jurisdictions'. Businesses in the financial sector may in the future be pressured by government to install biometric security measures.

BIOMETRICS, IDENTIFICATION, SECURITY AND BUSINESS PRACTICE.

Biometrics is the use of technology to recognise individual human features such as fingerprints, retinas and hand prints. That is, a computer can be programmed to identify an individual by recognising an individual's thumbprint. As each human's fingerprint is considered unique the use of a thumbprint as a means of identification has significant security advantages. A thumbprint cannot be forgotten and is unlikely to be lost or misplaced. This is the case with other personal attributes such as retinal scans. Criminals may chop off fingers and thumbs to gain access but this does not guarantee access because many scanners can be programmed to check temperature.

Computer technology offers an ideal tool by which biometric traits can be utilised for security purposes. Businesses that need to limit access to buildings and/or computer systems or identify those who access computer systems should carefully evaluate whether or not the use of biometric authentication provides the appropriate security needed for the assets to be protected. Biometric authentication offers enhanced security, but brings associated privacy issues.

The uniqueness of biometric identifiers is both a strength and a weakness. The strength lies in the ability to limit computer network system access to only those persons whose thumbprint has been validated. The weakness is twofold. Firstly, there is no guarantee that someone who has been accessed as reliable and granted access via biometric authentication will remain loyal. Secondly, there is a resistance to the use of biometric authentication as an access tool because of privacy concerns , the association of fingerprint identification with criminal activity , misuse of the fingerprint reference data and/or misuse of the information that links the fingerprint to an individual. Nonetheless biometric authentication is an enhanced security protection device .

The technology needs not only to protect the stored personal data that underpin biometric authentication, but also the biometric image that is unique to each individual. Enhanced protection can be gained by use of a

mixture of security techniques . The most common authentication procedure is via passwords. Financial institutions often require two levels of authentication, a card and a password. Biometric authentication adds a third layer of authentication. Theoretically, the more layers the greater protection suggesting it is possible for biometric authentication to be implemented in a way that does not compromise individual privacy .

BIOMETRICS AND PRIVACY - THE GOOD NEWS.

Cavoukian notes that before biometrics will 'become a friend of privacy' stringent safeguards, 'both legal, procedural and technological' will need to be implemented . Overcoming privacy concerns is a hurdle for businesses seeking to enhance security via the use of biometric technology. For example, in a recent paper Dike-Anyiam and Rehmani (2006) investigated the main factors that affect the adoption of biometric authentication. While their study demonstrated a clear advantage for biometric authentication over password authentication, one of the concerns identified by 71% of the respondents was privacy . The authors found that the more people are concerned with privacy the less likely they are to adopt the biometric authentication technology .

It is this concern about privacy that the Ontario Privacy Commissioner (Ontario, Canada) believes has been overcome through negotiation with government. In essence, privacy is protected by a combination of technology and legislation. In Ontario, Canada, the original biometric data must be encrypted, the original destroyed, the encrypted data and/or the biometric identifier must be held within a system that cannot be linked to other databases. Only encrypted biometric data are to be stored or transmitted and the system has to be constructed so that it will be impossible to reconstruct the original biometric from the encrypted biometric data . The appendix to Cavoukian's article contains the relevant sections of the Social Assistance Reform Act concerned with biometric information.

In addition, there has been a steady development in privacy-enhancing technologies (PETS). The key to PETS is strong encryption allowing individuals to keep their communications and their identities confidential . While the commissioner concludes that it is feasible and desirable that a privacy architecture is created for the 21st century, the reality will not be so easy . Bleumer proposes a cryptographic solution for maintaining individual privacy. The crux of his system lies in the use of pseudonyms and cryptographic building blocks. While the system appears to enhance privacy it still requires the use of linked technology, assumes the original biometric data cannot be linked back to individuals regardless of use patterns, and uses a pseudonym which can be linked to an individual.

BIOMETRICS AND PRIVACY - THE NOT SO GOOD NEWS.

Biometric data can be used reliably to recognise individuals quickly, anywhere, and at any time throughout their entire life . Once deployed on a wide scale individuals will find that biometric recognition becomes the default and avoiding it will require criminal activity . In addition, some biometric data will allow medical evaluation, for example; retinal scans in which there is a branch of 'medicine' known as iridology that seeks to identify health problems through observations of the eye and its components. This will have implications for businesses because of the potential impacts on insurance and it may also affect individual employment options.

Some researchers distinguish between biometric authentication and biometric identification on the basis that the former is no threat to individual privacy because control over the biometric data stays with the individual. This can be effectively countered. Individuals can be identified when they use biometric authentication as demonstrated earlier with Google wherein computer systems keep a log of individuals or what biometric reference accessed computer network systems and in particular what information was sought. The fact that your fingerprint is used to access a computer network system will almost certainly be recorded even if the system has no data on you . The same happens with passwords, but biometric authentication limits access to the holder of a fingerprint which is authenticated. Subject to false acceptances or the use of a severed finger there will be no doubt who accessed the system. Where now an individual might use several passwords, biometric technology eliminates the need for multiple passwords and should computer systems be linked authentication will mean

identification. For businesses this has clear advantages; for individuals the problems of remembering passwords may be replaced by, amongst other things, the potential of greater effective surveillance.

Consider also what happens if the system fails to recognise/authenticate the individual or mistakes one biometric for another, both feasible and possible . If there is no database holding an 'original copy of the biometric' or even an encoded digital scan then individuals will have to re-present themselves for authentication and start again. If there is an 'original or encoded copy' the individual will still have to re-present to determine the cause of the error or mistake. Even when systems promote privacy enhancing features the reality can be quite different. For example; van der Ploeg recounts an interview with an inspector at Los Angeles Airport about the hand geometry-based system used in INSPASS, a system used to enable frequent travellers to pass quickly through immigration. Although

> the functionality of the system did not require central storage of the biometric data after issuing the card, I was told that whenever someone would lose or damage their card, a new one could be sent by mail without the person having to come to an INPASS enrolment centre to register again. 'So, yes, that must mean we keep the biometric data somewhere in here as well' .

Even assuming a business is able to encrypt, convert a biometric to a template and store securely, this does not guarantee privacy even if assurances are given that what is stored is irreversibly changed. Tomko notes:

> I want to point out that even if the actual fingerprint pattern is not stored, but only a digital template is stored which cannot be converted back to the original fingerprint pattern, you still have the same problem. If the police obtain access to a similar scanner, tap into the output of the camera in the scanner, and place some digitized latent fingerprints through the system, they will generate a similar unique template within the accuracy limits of the system .

Tomko claims that the use of a template makes little difference because both original fingerprint and corresponding template are 'unique identifiers of an individual' and are 'traceable surrogates of my real identify' .

On a more fundamental level, businesses need to be wary of relying solely on fingerprint biometrics. Problems occur because of work practices, physical disability or physiology . Biometric fingerprint trials conducted by the United Kingdom Passport Service found about 80% of the sample population achieved successful fingerprint verification during trials . Businesses need to ensure they have simple and effective fallback procedures when problems occur with biometrics.

BUSINESSES – COMPULSORY IDENTIFICATION AND REPORTING.

International and domestic responses to terrorism have resulted in Australian financial institutions becoming deputy-sheriffs in the 'war on terror' locally via the requirements of the Financial Transactions Reports Act. The 100 point identification test was only the first step. Financial institutions will be required to apply a risk-based approach to customer interactions identifying and reporting customers who trigger pre-determined criteria. This already exists with cash transactions of A$10,000 or more. A future trend will almost certainly be incorporating electronic verification of all customer transactions so that the State can more easily monitor individuals determined to be at risk. Privacy legislation does not stop government agencies from conducting surveillance on citizens and accessing data held by businesses on citizens.

BUSINESSES – MATTERS THAT IMPACT ON PRIVACY AND BUSINESS PRACTICE.

Cultural differences:

Businesses considering the introduction of biometric authentication might also care to take into account world events and cultural differences. The latter is highlighted by a study on the introduction of smart card technology in Hong Kong and Ontario, Canada. These smart cards contain, amongst other things, personal data about an

individual. Bailey and Caidi highlight the different understandings residents of Hong Kong and Ontario, Canada hold as to what constitutes privacy, for example, the importance of anonymity . Their study found that while the former readily adopted smart card technology holding personal data, the latter have not been so keen. The differences can be partly explained by history. That is, Hong Kong residents have carried identity type cards for decades. Furthermore, Chinese people have a different cultural perspective, not possessing a strong concept of privacy whilst favouring recognition as important . However, one reason advanced for the ease of introduction was the extensive consultation process the government entered into with the residents of Hong Kong . In Ontario, Bailey and Caidi (2005) found citizens were disturbed about organisations tracking their activities, habits and personal information. Considering the level of governmental control over Chinese within the People's Republic of China the residents of Hong Kong may come to regret their enthusiasm for smart card technology that links personal data to immigration, electronic certification for virtual transactions, library card and driving licence type applications despite existing privacy legislation.

International influences:

The second, a world event, caused fundamental reappraisals of what is private. The events of September 11, 2001 resulted in a widespread loss of privacy for anyone travelling to the United States of America even though just about everyone who travels there is not and never will be a threat to American security. Air travel has become more personally invasive with physical body scans, touching, removal of items of clothing and in some cases questioning as part of ion scans. Some of these existed before, but in the context of drug smuggling although with drugs authorities have to have a suspicion that an individual is a drug carrier. Following September 11, all travellers are suspect and for the common good, citizens accept these new procedures as part and parcel of modern day travel.

The perception at the borders to the United States is that everyone is a threat to national security. To enter the United States nearly everyone has to comply with the Department of Homeland Security requirements known as US-VISIT. This means having two index fingers fingerprinted, a digital photo taken and travel documents scanned. Students entering the United States of America are subject to Student Exchange Visitor Information Service (SEVIS) requirements and their details and attributes are widely circulated to law enforcement organisations and their educational institution. One of the SEVIS websites extends the reach of the department of homeland security by simply stating 'anyone using the system expressly consents to monitoring'(SEVIS).

The implications for visitors should there be a mistake would be profound and serious. Computer systems malfunction, people tell lies for reward or to avoid trouble, sometimes mistakes happen and an individual could experience 'potential statelessness' .

Australia responses to terrorism that impact on business practice:

In Australia, recent anti-terrorism legislation has prescribed terrorism, defining a terrorist act widely (s.100 *Criminal Code Act 1995* (Cwlth)). Businesses need to recognise the extent of the legislative change with government now having the power to proscribe an organisation a 'terrorist organisation' effectively making its members terrorists. Legislation has tossed aside traditional common law rights such as a right to silence, unrestricted access to a lawyer of choice and freedom of speech (ss.34G, 34TA and 34NVAA *Australian Security Intelligence Organisation Act* 1979 (Cwlth) (ASIO Act)). For example: The ability to classify an organisation as a terrorist organisation means its members may have, by being members of a proscribed organisation, committed an offence (s.102.1 *Criminal Code*).

Businesses in Australia need to take account of the implications of s.37 ASIO Act that allows for security assessments to made concerning persons and s.102.2 *Security Legislation Amendment (Terrorism) Act 2002* (Cwlth) which allows the Attorney-General to proscribe organisations that are involved in, linked to or associated with terrorist activities. Financial contact between persons and terrorist organisations has been prescribed (ss.102.6, 103.1 Criminal Code). The definition of 'terrorist activities' is wide, encompassing industrial and

political dissent. In 2005 these powers were extended to include organisations that advocate the doing of a terrorist act (ss.102.1, 102.1(2) *Criminal Code*). Furthermore, s.34F(8) *ASIO Act* provides for incommunicado detention of persons without notification by agents of ASIO. In New South Wales, the Carr Government passed the *Terrorism (Police Powers) Act 2002* (NSW) which in s.13 removes from scrutiny by any court except the NSW Police Integrity Commission any decision of the Police Minister. While these changes were heralded as the new bulwark against terrorists they also impact upon business practice. For example, businesses may be required to produce documents, information and things which could include biometric data on persons with whom they do business and hold as clients or employees (*Anti-Terrorism Act (No 2) 2005* (Cwlth)). Of particular concern is the acquiesce of some major media outlets who promote discarding traditional legal protections because someone is associated with terrorism .

These all represent a real and present added risk to businesses and institutions seeking to incorporate enhanced security measures to protect computer networks because some of these systems will hold data and information of interest to governments and security agencies. A claim of privilege or privacy by a business over its information databases on citizens will fail if the request is terrorist linked (s.201A of Schedule 2, *Cybercrime Act*). New laws also provide agents of ASIS and DSD access to computer networks, require persons subject to a warrant to produce things (s.34G(3) *ASIO Act*). Appeals to public opinion will almost certainly be illegal as legislation provides for secrecy surrounding warrants and questioning (s.34VAA *ASIO Act*). Businesses should not expect support from some major Australian newspapers, in particular the national daily The Australia newspaper, which on recent performance, may well ridicule any business seen to be soft on terrorism .

THE FUTURE

Predicting the future is always fraught with risk. However, there are several identifiable risks. Cyber crime will increase thereby placing a greater burden on businesses to protect business assets along with the data businesses hold on clients and users of business n computer systems. Computer technology will continue to develop as will requirements for enhanced security options, including those offered by biometrics. Concepts of what is private and what we, as individuals, can keep private will also change. Changes in recent international travel give a good indication. To board an aeroplane involves at the very least a body scan and can also involve removal of clothing and personal handling by airport security staff. This is non negotiable. To enter the United States of America passengers have, at the very least, two fingerprints taken. This is non negotiable. A successful terrorism event in Australia linked to overseas interests will result in tighter security at points of entry and exit. What the war on terror has done is to lower resistance to personal searches and the taking and storing of personal information by the authorities. This is changing personal concepts of what is private. Whether or not there will be acceptance of universal biometric authentication procedures, only time will tell. However, unless Australians are careful the use of widespread biometric identification will creep up on them.

Businesses can utilise this lowered resistance to searches and questioning to introduce biometric authentication/identification technology if they can provide adequate privacy protections regardless of government's legislation. Businesses do this by clearly identifying the appropriate level of security needed for computer access and for entry to buildings and rooms. Biometric authentication should be restricted to computer networks and buildings requiring a very high level of security and as such should be the end of a sequence of security measures, not the only security measure. In other words, biometric identification procedures should be limited to those that need it, not promoted as a general panacea for security problems. Businesses need to employ the best safeguards, including encryption technology and highly restricted access to biometric authentication data. Use of this data should be confined to the initial security purpose unless informed approval is given in writing by individuals whose biometric data are held. Finally, businesses that use or institute biometric authentication procedures need to warn both employees and clients of the added loss of privacy risks that come with the use of this unique identifier in our modern and changing world. Fighting cyber crime brings with it the risks of being caught up on the war on terror and all the security concerns that go with terrorism.

REFERENCESLEGISLATION

Anti-Terrorism Act (No 2) 2005 (Cwlth)

Australian Security Intelligence Organisation Act 1979 (Cwlth)

Criminal Code Act 1995 (Cwlth)

Cybercrime Act 2001 (Cwlth)

Financial Transactions Reports Act 1988 (Cwlth)

Privacy Act 1988 (Cwlth)

Privacy (Private Sector Amendment) Act 2000 (Cwlth)

Security Legislation Amendment (Terrorism) Act 2002 (Cwlth)

Terrorism (Police Powers) Act 2002 (NSW)

ACKNOWLEDGMENTS

I would like to thank Dr Ann-Claire Larsen for reviewing the paper and her constructive comments on construction, prose and grammar.

COPYRIGHT

Michael G Crowley ©2006. The author assigns Edith Cowan University a non-exclusive license to use this document for personal use provided that the article is used in full and this copyright statement is reproduced. The author also grants a non-exclusive license to Edith Cowan University to publish this document in full in the Conference Proceedings. Such documents may be published on the World Wide Web, CD-ROM, in printed form, and on mirror sites on the World Wide Web. Any other usage is prohibited without the express permission of the author.