PRIVACY INTERNATIONAL

Assessing Biometrics and Privacy and Touching Big Brother

Archived report by Privacy International
July 1996

Abstract

The evolution of information technology is likely to result in intimate interdependence between humans and technology. This fusion has been characterized in popular science fiction as chip implantation. It is, however, more likely to take the form of biometric identification using such technologies as fingerprints, hand geometry and retina scanning.

Some applications of biometric identification technology are now cost-effective, reliable, and highly accurate. As a result, biometric systems are being developed in many countries for such purposes as social security entitlement, payments, immigration control and election management. Whether or not biometry delivers on its promise of high-quality identification, it will imperil individual autonomy. Widespread application of the technologies would conflict with contemporary values, and result in a class of outcasts.

The author

Simon Davies is Visiting Fellow in the Department of Law, University of Essex, United Kingdom; Visiting Fellow in Information Law at the University of Greenwich, London; Consultant Advisor to the British Medical Association; and Director General of Privacy International, London, UK

PRIVACY INTERNATIONAL

Table of contents

Introduction	4
Biometric technologies	6
Case studies	8
The achievability of biometrics' potential benefits	11
The dangers of biometric identification	12
Conclusions	14
References	15

Introduction

The accurate identification of individuals is a key concern for many government agencies and corporations. It is important to them because it contributes significantly to administrative efficiency and the control of fraud, and can offer benefits to clients as well. A key focus of information systems security in recent years has been the intensification of efforts to establish accurate identity.

The application of identification systems involves conflict between two conditions. On the one hand, flawed identity checking results in unnecessary duplication, fraud, and client disruption, with resultant costs and risks; and on the other, a rigorous identification procedure is invasive, and its effectiveness may be undermined by unpopularity and resultant falsification and evasion.

Three conventional forms of identification are in use today. The first is something you have, such as a card. The second form is something you know, such as a password or PIN. The third is something you are, such as a pattern of ridges on a fingertip; or something you do, such as writing or speaking. This third form of identification is known as 'biometrics'.

Schemes based on the items and knowledge which people possess have many weaknesses. For example, fake 'blanks' of even the highest integrity cards are generally available in East Asian countries within weeks of the first cards being issued (Davies 1992a, p.42). The general availability of sophisticated manufacturing equipment has placed the ability to forge such documents into the hands of a much wider group of criminals than was previously the case (Carroll 1991, pp. 10-13).

A high-integrity biometric system appears, from the perspective of information users, to be an ideal solution to such problems. The development and application of technical standards has meant that communications among the information systems of different organisations is increasingly simple. The application of a biometrically-based identifier for each individual would be a natural further step.

Yet, from the perspective of individuals, any move towards a biometric identifier carries enormous risk. Many systems do not live up to expectations because they prove unable to cope with the enormous variations among large populations, or fail to take into account the practicalities of human behaviour, and the needs of people. Individual autonomy and freedoms may be compromised by the need for a high level of compliance with the scheme. In many western nations, the stigma of criminality is associated with fingerprinting, and, by association, with other biometric techniques. If a scheme is applied across multiple organisations, behaviour in relation to one organisation might lead to a domino effect of 'cross-enforcement' activities, involving suspension of entitlements or benefits by other organisations. Individuals who cannot, or will not, use the prescribed system may become outcasts on the edge of society.

The purpose of this paper is to present an overview of biometric systems, and discuss the justifications for its implementation and the dangers inherent in them. Because biometric technologies, their application, and their working environment are all in their infancy, the research on which this paper is based has relied heavily on case studies, literature search, primarily in the popular and trade press, and interviews with leading figures in the field. Where applicable, studies and working documents have been incorporated.

Biometric technologies

Biometrics has been applied in a variety of ways since at least the time of the Pharaohs, who used height measurement. Automated biometric technology was first applied in controlling access to premises and to computer networks. Modern biometric schemes generally rely on sophisticated computer scanning technology, of such aspects of the body and its behaviour as the micro-visual pattern on the retina, the geometry of the hand or a finger, the patterns on the surface of the skin of the thumb or fingers, the aural pattern of the voice, the pattern of handwriting or signatures, and facial appearance. In each case, an artifact analyses a sample presented to it, and compares the measurement with a verified sample digitally stored in the system.

In recent years, biometric technology has attained a very high degree of sophistication, and accuracy has been achieved at a level which far surpasses all other forms of identification. The Iriscan system, for example, conducts a scan of the eye, and, according to claims made by the manufacturer, is generally accurate to 1015 on the first scan, and 1022 on the second (BTT 1993a). Iris recognition does, however, suffer from the shortcoming that many people feel very sensitive and protective of their eyes, and find such technology disquieting. To address at least some of this concern, research is currently underway to scan the eye at a range of up to three meters.

Currently the most popular form of biometry is fingerprinting. National computerised fingerprint systems exist in several countries, the first national system having been established in Australia in 1987. The Japanese telecommunications giant NTT recently announced the development of a fingerprint recognition method that it claims provides further improvements in speed and accuracy. Recognition of a fingerprint takes place in an average of 2 seconds on a personal computer or 1 second on a workstation, with accuracy claimed to be above 99.9%. Among its diverse potential applications, it could be used to confirm that the bearer of an identification card is the person to whom it was issued (TA 1993). Meanwhile, the Biometric Technologies Company of the U.S.A. is developing a fingerprinting system using neural networks. Laboratory tests commissioned by the manufacturer are reported to show an accuracy of 0.0001% and a probability of wrongly rejecting a genuine client of 0.1%. Known as Printscan 3, the device is intended for release in the early part of 1995 at a cost of $US600 per unit (BTT 1993b).

Hand geometry, involving a scan of the shape and characteristics of the entire hand, has been applied in a variety of situations in over 4,000 locations including the Colombian legislature, the San Francisco International Airport, a day care centre at Lotus Corporation in the U.S.A. and a Los Angeles sperm bank (Miller 1994, p.25).

Evaluation of biometric technologies will be essential to their acceptance, but to date only limited independent testing has been undertaken. In 1991, the U.S. Department of Energy's Sandia National Laboratories released the results of its second round of tests. The significance of these results remains open to question, however, since they assessed equipment from only six U.S. vendors: Indentix's Touchlock fingerprint system, Recognition Systems' ID-3D-U hand geometry system, Eyedentify's Model 8.5 retinal scan system, Autosig's Sign/On signature dynamics system, and Alpha Micro's Ver-a-tel and International Electronics' VoiceKey voice verification systems (Sherman R.L. 1993).

The tests showed that dynamic signature verification was by far the cheapest of the evaluated products, although it rejected a high proportion of properly enrolled individuals. Hand geometry had a very low rate of false rejections, especially if more than one attempt was made, and was very much better than signature dynamics in this respect; however it cost more than twice as much.

Case studies

In order to provide some depth of understanding of the nature of biometrics-based identification, this paper documents several schemes. The first is a single-purpose scheme in pilot operation, and the second a multi-purpose system currently under development. Several other applications are identified.

National border crossings

In 1993, the U.S. immigration authorities opened a new lane at New York's John F. Kennedy airport. It differs from traditional immigration procedures in that it uses biometric technology called FAST (Future Automated Screening for Travellers) to automatically identify and process passengers in as little as twenty seconds.

The project is called INSPASS (Immigration and Naturalisation Service Passenger Accelerated Service System). Applicants for registration are interviewed, and their identity confirmed. They place the palm of a hand onto the surface of a scanner, which records measurements of the hand's contours. These are converted into a 'template' and stored on a card. This is currently a paper card, but is soon to be a 'smart card'. In case the hand geometry system proves to be inadequate, fingerprints are also taken and recorded.

When INSPASS members arrive at the two test airports (John F. Kennedy and Newark), they bypass the main immigration queues, and enter a kiosk. The card is presented to the terminal. The hand is placed onto a scanner, which matches the biometry of the hand with the template encoded into the card. Immigration databases are consulted. Once the last of five green lights appear at the tips of the fingers, the glass exit door opens, and the passenger continues to the baggage claim and customs zone.

INSPASS is currently operating as a voluntary system for frequent travellers to and from the U.S.A., who are U.S. or Canadian nationals, or nationals of countries involved in the U.S. visa waiver scheme. More than thirty thousand people have so far enrolled, and by mid-1994 this was increasing by one thousand per week. Governments in 26 countries are monitoring and cooperating with the project (BTT 1993b, Davies 1994b).

If the INSPASS trial is successful, the technology may render conventional identification card and passport systems redundant. As a trade-off for faster immigration processing, passengers are accepting a system which has the potential to generate an increased amount of international traffic in their personal data. INS officials appear confident that a multi-purpose scheme can be established, using common international standards and a smart-card system that can cope with either a hand geometry or a fingerprint scan. Immigration control could be linked to a wide spectrum of information, such as police and taxation systems.

The system has been approved by a preliminary feasibility audit, and looks increasingly like being implemented in several countries. The trial may be the forerunner of a linked biometric system that involves many nations.

Social welfare

In the Canadian province of Ontario, there is considerable public concern about the existence of nearly twelve million identities in the health system of a province with a population of ten million. It is perceived that many U.S. citizens are using Canadian health care facilities without entitlement. To address the problem, the provincial government is developing a proposal for a government-wide biometric scheme variously called the Ontario Client Positive Identifier Proposal or Service Card Ontario. It is being championed by the Community Services Department of Metro Toronto, an agency which disseminates around $Can2 billion ($US1.4 billion) per annum in welfare services.

A committee representing the majority of Ontario Departments is currently discussing mutual identification and administration problems, and the potential for creating a universal strategy for dealing with these issues (Davies 1994a). Officials are hopeful that a register of thumb scans can be established by 1996 as the basis for a 'once-and-for-all' identity. Scanners would be located at many locations in all Ontario Government agencies, and connected to a thumb-scan registry and to the computers of relevant agencies. Discussions are underway with Federal agencies with regard to integration with immigration systems.

The Request For Information (TMS 1993) envisaged that the system would involve:

- digitised photographs and hand geometry stored in a central database;
- a plastic identity card, possibly with a magnetic strip, containing facial image, client signature, client date of birth, a variety of security features, and possibly a fingerprint;
- authorised users at multiple sites using data scanned from a person's hand to search the databank for matches; and
- interfaces with existing information systems.

Five of thirteen companies providing submissions were shortlisted. The principal difficulty for suppliers appeared to be the capability to interface with existing technologies. A Request For Proposal was subsequently issued (TMS 1994). The total cost for hardware, software, maintenance, training and peripherals was indicated to be in the range of $Can3-4 million. According to project staff, this expenditure would be recovered from administrative and payments savings. The project team recognises that there are significant administrative barriers, but hopes to overcome them.

The Department has announced that it intends pursuing a policy of 'openness and honesty' in the development of the system, and will appoint an external adviser to monitor its performance and impact. The Privacy Commissioner for Ontario, however, has had minimal involvement to date, and has expressed grave reservations about it. Issues of identification are still divisive in Canada (Phillips 1994), and the pursuit of the project may require considerable political will.

Emergent applications

Reports in the trade press suggest that biometric systems are being developed for a wide spectrum of purposes. Major retail and banking organisations in Australia, Europe and North America are adopting biometric systems for internal security. Blue Cross and Blue Shield in the U.S.A. have plans to introduce nationwide fingerprinting for hospital patients. This may be extended into other medical applications. The Jamaican Government is planning to introduce electronic thumb scanning to control elections. Social Security verification using biometrics is being planned in several countries including Spain and South Africa (BTT 1994a, 1994b).

In 1994, the U.K. Department of Social Security (DSS) developed a proposal to introduce a national identification card, which it is hoped will assist in reducing the estimated [[sterling]]1 billion of welfare fraud annually. The DSS recommended a computerised database of hand-prints of all of the 30 million people receiving a government benefit. Applicants for a benefit or subsidy would have their hand-prints tested against existing entries (Sherman J. 1993). The proposal is expected to be one of the options contained in a Green Paper on an identification card, to be released in the Spring of 1995.

In Europe, tests are being undertaken of the feasibility of storing card-holders' fingerprints on their credit cards, so that a device at the point of purchase can compare the card-borne data with the bearer's fingerprint. In Australia, the technology is being applied to staff who access automated teller machines. Government officials in The Netherlands say that biometrics has a "real chance" of being accepted as a form of identification. According to the Chip Card Platform, which is coordinating the project, there has been a political 'change of wind' in recent years, and an understanding amongst the public of the role of information technology. Officials acknowledge that this change of attitude has taken them by surprise (Davies 1994a).

The achievability of biometrics' potential benefits

The potential benefits of an integrated biometrics-based identification system include improvements in:

- the cost of administration;
- the integrity of identification;
- the integrity of information;
- access to information held by organisations;
- the speed of delivery of services and benefits;
- the accuracy and quality of research and statistics; and
- the level of technical security of communications.

In many countries, information technology is being successfully applied to particular business and administrative functions within particular organisations. The majority of these success stories have in common a manageable size, a limited geographic spread, a single purpose, and modest and easily defined goals. Where biometric technologies are applied to specific purposes, some confidence may be felt in the system's ability to deliver the intended benefits.

On the other hand, many failures and disappointments continue to occur, even among seemingly straightforward projects. A report commissioned by the U.S. Department of Health and Human Services noted that a vast gulf exists between the promise and the reality of savings from computer systems (HHS 1993). A study by the Congressional Office of Technology Assessment found that computer-based information systems, once implemented, often result in "unforeseen costs, unfulfilled promises, and disillusionment" (OTA 1993).

Large-scale government schemes have been shown in several countries to be much less cost-effective than was originally estimated. Years after the governments of the United States and Australia developed schemes to match public sector data, there is still no clear evidence that the strategy has succeeded in achieving its goals. The audit agencies of both federal governments have cast doubt that computer matching schemes deliver savings. Achieving the potential benefits of large-scale applications of information technology is difficult, and the outcomes are erratic, unpredictable, and commonly considerably less than expected.

Complex systems embody greater levels of risk of failure, and resultant vulnerability of organisations and individuals dependent on them. An example of this was the shutdown of more than half of AT&T's network due to a computer virus in the network switching system (Davies 1990). The greater the complexity of a system, the more permutations of failure appear to be created. The case for multi-faceted integration of complex personal information systems, whether or not based on biometrics, must be viewed with some skepticism.

The dangers of biometric identification

The pursuit of high-quality identification involves significant technical, organisational, social, legal and political issues. Many of the these are concerns about computerisation in general, and the sharing of data among organisations in particular. For a review of the dangers of data surveillance to individuals and society, see Clarke (1988).

Biometric identification relies on technology that is far from proven, and major organisational adjustments are needed to cope with it. There are many practical problems involved in complex and largely automated schemes, and in coping with exceptions, system outages and claims of database error. The imposition of intrusive identification procedures changes the nature of relationships and transactions between clients and organisations. There is at least a perceived, and probably a real, increase in the power of organisations over individuals. Biometrics, much more so than other identification schemes, may imperil the sense of individuality.

Systems that entail a central registry of personal identities raise much more substantial issues. The adequacy of data protection laws in dealing with these issues to the satisfaction of the public is in doubt. A biometric print may, for example, be considered to be in the public domain. Alternatively, people may find that they are required to provide a biometric print in many unforeseen or unintended future circumstances.

The history of identification systems throughout the world provides evidence of ‘function creep’ - application to additional purposes not announced, or perhaps even intended, at the commencement of the scheme. Uses of the Social Security Number in the U.S.A, the Social Insurance Number in Canada, the Tax File Number in Australia, the SOFI number in The Netherlands, and the Austrian Social Security Number have been extended progressively to include taxation, unemployment support, pensioner benefits, and in some cases health and higher education. The existence of a relatively high-integrity scheme would create irresistible temptations to apply it widely, and inter-relate many hitherto separate collections of personal information (Holvast 1991, Clarke 1992, Davies 1992a).

Privacy protection involves resistance to the establishment or consolidation of monolithic information systems. Informational chaos and functional separation amongst agencies have ensured that the individual has not become a servant to the state. Variety, choice, and chaos have also had the effect of insuring the free movement, rights, and free choice of individuals against errors in the system.

Several countries, including Australia, Canada, the United States and New Zealand, have witnessed public disquiet over identification schemes. Abstract fears that have been cited include :

- that people will be de-humanised by being reduced to codes;
- that the system will enhance the power over individuals of particular organisations and the State;
- that high-integrity identification embodies an inversion of the appropriate relationship between the citizen and the State;
- that the system is a hostile symbol of authority;
- that society is becoming driven by technology-assisted bureaucracy, rather than by elected government;
- that exemptions and exceptions will exist for powerful individuals and organisations, and that the system will entrench fraud and criminality; and
- that such idwentification schemes are the mechanism foretold in religious prophecy (e.g. 'the Mark of the Beast').

There is some evidence that the public may be moving away from traditional notions of privacy, and cautiously accepting fraud control and administrative mechanisms that would have been politically untenable in the 1970s and 1980s. For example, both the Dutch and Australian public rejected national information and identification schemes en masse several years ago, but have reacted more passively to equally intrusive (though less blatant) schemes in the 1990s. In Germany, where the introduction of an identity card caused major controversy fifteen years ago, the public now appears to be more willing to accept a national 'smart card' scheme for the health sector.

There may be many factors at work in the apparently greater public acceptance of privacy-invasive schemes. Proposals are being brought forward in a more careful and piecemeal fashion, which may be lulling the public into a false sense of security. There is increasing popularity of computers and networks for personal use. The use of personal information systems by Nazi Germany to enable the identification and location of a target race are becoming a vague memory.

It is an open question, however, as to whether public acceptance is real, or only apparent. A change of attitude may merely await a catalyst. Alternatively, an increasing proportion of people may ignore official processes and organisations and opt instead for 'black markets' and 'black society'. Many countries have substantial sub-cultures of outcasts, usually resulting from poverty, racial differences or illegal immigration. To these may be added a significant number of people who choose not to participate in a general identification scheme.

Conclusions

Biometry is, in many senses, a natural extension of technological evolution. Like the modern automobile, it signals an intimacy with the client. Whether the public senses a danger in the establishment of such a fusion will depend on its sensitivity to privacy and autonomy.

High-quality identification offers the promise of the avoidance of error and fraud, and privacy advocates often have difficulty expressing their opposition to it. Nevertheless, the use of biometrics needs to conform to the standards and expectations of a privacy-minded society. Specific-purpose biometric schemes raise serious issues which need to be addressed. General-purpose schemes represent real threats to the fabric of contemporary society.

References

BTT 1993a Biometric Technology Today, London 1, 3 (June 1993)

BTT 1993b Biometric Technology Today, London 1, 7 (November 1993)

BTT 1994a Biometric Technology Today, London 1, 9 (February 1994)

BTT 1994b Biometric Technology Today, London 2, 3 (June 1994)

Carroll J.M. (1991) Confidential Information Sources, 2nd edition, Butterworth-Heinemann, New York, 1991

Clarke R. (1988) 'Information Technology and Dataveillance' Commun. ACM 31,5 (May 1988). Re-published in C. Dunlop and R. Kling (Eds.) 'Controversies in Computing', Academic Press, 1991

Clarke R. (1992) 'The Resistible Rise of the Australian National Personal Data System' Software Law Journal, 5,1, January 1992

Davies D. (1990) 'Anatomy of a disaster' Computer Law and Security Report Jul-Aug 1990

Davies S. (1992a) 'Big Brother: Australia's growing web of surveillance', Simon and Shuster, Sydney, 1992

Davies S. (1992b) 'Vulnerability reaching its elastic limit', in 'Managing information technology's organisational impact' Eds. Clarke R. and Cameron J., Elsevier Science Publishers B.V. North Holland, Amsterdam, 1992

Davies S. (1994a) 'Too many bytes to swallow' Report to the British Medical Association on Information Technology, London, 1994

Davies S. (1994b) 'Forget the passport, let's see your hand' The Independent, August 15, 1994, London

HHS (1993) 'Toward a national health information infrastructure', Report to the Secretary, US Department of Health and Human Services, Workgroup on Computerisation of Patient Records, Washington DC, April 1993

Holvast J. (1991) 'Vulnerability of Information Society', in Managing Information Technology's Organisational Impact, Eds. Elsevier Science Publishers B.V. North Holland, Amsterdam, 1991

Miller B. (1994) 'Vital Signs of identity' IEEE Spectrum, Institute of Electrical and Electronic Engineers, New York, February 1994

OTA (1993) 'Protecting Privacy in Computerised Medical Information' Office of Technology Assessment, US Government Printing Office, Washington DC, 1993

Phillips B. (1994) Privacy Commissioner of Canada, Annual Report, 1994

Sherman, J. 'Lilley considers using palm prints to vet pensioners', The Times, London, October 26, 1993

Sherman, R.L. (1993) Journal of Electronic Defense, January, 1993 Biometrics futures; EW Design Engineers' Handbook & Manufacturers Directory

TA (1993) 'NTT Develops Rapid, Highly Accurate Fingerprint Recognition Technique' New Era Japan, Telecommunications Association, August 15, 1993

TMS (1993) 'Request for information' Toronto Metro Services, Community Services Department, 1993

TMS (1994) 'Request for Proposal' Toronto Metro Services, Community Services Department, 1994