THE INTERNATIONAL PRIVACY BULLETIN
PUBLISHED BY PRIVACY INTERNATIONAL

VOL 4 NO 2 SPRING 1996

IN SEARCH OF PERFECT IDENTITY

SIMON DAVIES

The accurate identification of individuals has always been a key concern for governments and private sector organizations. The development of identification systems is important to organizations because it offers one contributing solution to fraud and administrative inefficiency. Such initiatives can offer benefits to the client as well as to the administration. For these reasons, all organizations strive to achieve "perfect identity" of their clients.

Conventional forms of identification have always been subject to fraud and manipulation. Card systems are the most vulnerable. Fake "blanks" of even the highest integrity cards are generally available in Singapore or Thailand within weeks of issue.[1] The general availability of sophisticated computer machinery has placed the ability to forge such documents into the hands of a much wider group of criminals than would have been the case in earlier years.

One of the largest problems facing benefits organizations, however, is the existence of multiple identities. Since most card systems rely on a pre-existing numbering or registration system, problems in the pre-existing system will be compounded.

Many current number systems are inadequate. The Social Security Number (SSN) in the United States has become a defacto national identifier, despite admissions by the Social Security Administration that between four and ten million false or illegal numbers are in circulation. In Ontario, nearly twelve million Health Benefits Cards have been issued to a population of ten million. The government of Sweden, which instituted the first national number fifty years ago, is now claiming that the system facilitates fraud. Limitations are now being set on the uses of the number, and the Swedish Data Inspectorate is moving to break the number's "monopoly". Authorities in Australia have detected forged Tax File Numbers since their inception, and although internal studies and estimates have been made, the ATO refuses to divulge these figures.[2]

The development of high integrity identity systems is, however, fraught with problems. An overly rigorous identification procedure could prove unpopular, forcing some people to drop out of the system, and inviting a degree of civil disobedience in others. On the other hand, lax and ineffective procedures leave organizations vulnerable to fraud. A key focus of

Continued on page 14

PRIVACY INTERNATIONAL OFFICE BEARERS

DIRECTOR GENERAL

Simon Davies
Computer Security Research Centre
London School of Economics
Houghton Street,
London WC2A 2AE
United Kingdom

Phone 44 81 402 0737 Fax 44 81 313 3726
Email: Davies@privacy.org

DEPUTY DIRECTOR

David Banisar
Electronic Privacy Information Center
666 Pennsylvania Ave S.E. Suite 301
Washington, D.C. 20003 U.S.A.

Phone 1 202 544 9240 Fax 1 202 547 5482
Email: Banisar@epic.org

SECRETARY GENERAL

Marc Rotenberg
Director
Electronic Privacy Information Center
666 Pennsylvania Ave S.E. Suite 301
Washington, D.C. 20003 U.S.A.

Phone 1 202 544 9240 Fax 1 202 547 5482
Email: rotenberg@epic.org

The International Privacy Bulletin (ISSN: 1071-6807) is published quarterly by Privacy International. All enquiries should be directed to:

Privacy International Washington Office
666 Pennsylvania Ave., SE, Suite 301
Washington, D.C. 20003 U.S.A.

Phone 1 202 544 9240 Fax 1 202 547 5482
Email: pi@privacy.org
http://www.privacy.org/pi/

Editor: David Banisar

Assistant Editor: Vicki Peterson

Contributing Editors: Simon Davies, Wayne Madsen, Marc Rotenberg.

ADVISORY BOARD MEMBERS

Professor Dr Jon Bing
Norwegian Research Centre for Computers and Law
University of Oslo
Niels Juels gate 16
N-0272 Oslo 2
NORWAY

Madeleine Colvin
Legal Officer
Justice Coalition
74 Chancery Lane
London WC1
UNITED KINGDOM

Graham Greenleaf
Senior Lecturer
Faculty of Law
University of New South Wales
PO Box 1
Kensington NSW 2033
AUSTRALIA

Attny Cecilia Jimenez
Deputy Secretary General
Philippines Alliance of Human Rights Advocates
Room 403 9 Balete Drive
Quezon City Metro Manila
REPUBLIC OF THE PHILIPPINES

Pierrot Peladeau
Vice-President, Research and Development
Societe Progestacces
P.O. Box 42029
Montreal, Quebec
CANADA H2W 2T3

Professor David McQuaid-Mason
Dean Faculty of Law
University of Natal
King George V Avenue
Durban 4001
SOUTH AFRICA

PRIVACY INTERNATIONAL

Not Such a Good ID

ID card proposals currently being considered by the United States, Britain and Canada have sparked a range of concerns throughout the political spectrum.

This edition of the *IPB* discusses the many issues that are raised when ID cards are introduced into a democratic nation. The implications are profoundly important and very complex. At the heart of the ID card notion is a shift in the relationship between citizen and state, and an increase in a range of official powers. Any move in this direction should be made only after serious and genuine public consultation.

The purpose of ID cards varies from employment and welfare entitlement to law enforcement, but there is surprisingly little documented evidence to justify claims made about the need for the cards. Few police or criminologists have been able to advance any evidence whatever that the existence of a card would actually reduce the incidence of crime, or the success of prosecution. Their impact on illegal immigration has not been quantified, and claims made about the benefit of cards in the fight against tax evasion are generally unreliable.

More to the point are the hidden dangers that an official ID card brings with it. The entrenchment and expansion of criminal false identity is rarely addressed by authorities anxious to sell an ID card to the public. The implications of creating an internal passport are generally ignored, as is the growing body of evidence that ID cards foster an endemic component of discrimination.

Virtually all countries with ID cards report that their loss or damage causes immense problems. Up to five per cent of cards are lost, stolen or damaged each year, and the result can be denial of service ad benefits, and - in the broadest sense - loss of identity.

All ID cards - whether voluntary or compulsory - develop into an internal passport of sorts. Without care, the card becomes an icon. Its use is enforced through mindless regulation or policy, disregarding other means of identification, and in the process causing significant problems for those who are without the card. The card becomes more important than the individual.

Privacy International has opposed the introduction of these cards in many countries. We do so because the existence of a card challenges important precepts of individual rights and privacy. At a symbolic and a functional level, ID cards are an unnecessary and potentially dangerous white elephant. They are promoted by way of fear-mongering and false patriotism, and are implemented with scant regard for serious investigation of the consequences.

THE INTERNATIONAL PRIVACY BULLETIN
Published by Privacy International

VOL 4 NO 2 Spring 1996

CONTENTS

U.S. LOBBIES OECD TO ADOPT KEY ESCROW

MARC ROTENBERG

Some commentators have suggested that the OECD may soon adopt key escrow encryption, favored by the United States. In this article, Marc Rotenberg suggests that the US is using the OECD in a last ditch effort to win support for Clipper.

It was the worst of times for Clipper encryption proponents. The communication surveillance scheme developed by the US National Security Agency and blessed by the White House had become a political embarrassment. Industry and civil liberties groups had banded together and ridiculed the plan. *The New York Times* reported that government crypto could be hacked. Even commercial key escrow, "Clipper Lite", wasn't selling.

The future looked even worse. Consumer demand for encryption was growing. Foreign competitors were offering good products. Congressional efforts to reform outdated export controls laws were gathering support. Funding for the digital telephony plan was in doubt.

Policy makers needed a new market for key escrow. It was time to launder domestic policy through international channels. It was time to take Clipper on the road.

Washington Leaves Washington

In 1994, key NSA and law enforcement officials packed their bags and went overseas. They lobbied US allies in London, Bonn and Brussels to adopt Clipper-like crypto. They warned incredulous Central and Eastern European officials that wiretap capability should be built in the new communications infrastructure.

They suspected that government escrow was not going to be a big sell, considering that electronic surveillance is more often about economic espionage and spying on trade negotiators and political opponents than stopping terrorists. But they gambled that a key escrow infrastructure, even one built by the private sector, would keep alive the possibility that at some point (a terrorist attack?) government could reassert total control over encoded communications.

The strategy also had the benefit of bootstrapping domestic policy. If the US was unable to get a bill through Congress mandating key escrow, perhaps it could push allies to embrace the plan then later return to Congress with tales about "growing US economic isolation" in a world of key escrow encryption.

Government Communications Headquarters (GCHQ) in London, which receives substantial funding from the NSA in Washington, signed on for the plan and lobbied the Home Office for a key escrow standard. The UK, always the closest ally to the US on all matters of espionage, became the bridgehead for the Continent. A former GCHQ official assigned to the European Commission in Brussels also pushed forward an escrow plan for the EU. But a few bilateral agreements would be too slow. The US needed a strategy to "escrowize" crypto before anyone caught on.

Washington Goes to Paris

Washington turned to the Organization for Economic Cooperation and Development in Paris. The distinguished group occupies a unique role in international policy. Without the financial resources of the World Bank or the military might of NATO, the OECD must rely on policy expertise and the good will of member nations to develop appropriate policies. It has played its role well. OECD reports provide the statistics, insights, and research that guide national governments on issues from agriculture policy to telecommunications reform.

The OECD also has played an increasingly important role in the recently established democratic governments of Central Europe. In 1995, the Czech

Republic became a member. Poland and Hungary joined in 1996. One of the central concerns of the OECD in Central Europe is to encourage the continued development of democratic institutions.

The OECD also has impressive hi-tech policy credentials. Distinguished international panels, led by well respected Australian jurist Michael Kirby, developed international policies for transborder data flows in 1980 and information security in 1992. The privacy policy became the basis for national law in more than a dozen European and Pacific rim countries. The information security guidelines were not easily translated into national law, but their influence is still recognized.

But when the OECD found itself looking for new projects after the information security study was completed, the US, a major funder of the organization then in arrears, had the answer: a new international policy for encryption. The topic was timely and renewed US interest in the OECD was welcome. The OECD had already begun a review of the issue. The OECD expert panel was quickly formed in Paris in December, 1995. A set of principles were drafted and discussed. Debate continued at a meeting in Canberra in February, 1996 and then in Washington, DC in May 1996. Further discussion is planned for late 1996. The outcome is still far from clear.

The OECD Comes to Washington

Many obstacles remain at the OECD for Clipper proponents. The OECD typically operates by a slow, consensus building process. Since the institution has no legal authority, and multiple political systems and cultural traditions must be brought together, every attempt is made to explore and analyze. National sovereignty is a sensitive issue.

Central to understanding the role of the OECD also is its commitment to democratic institutions. Indeed, to read the 1980 privacy principles is to be reminded once again that in democratic nations citizens have rights which governments must respect. Even the security policy, hardly the stuff of civics class, echoes the OECD's commitment. "The security of information systems should be compatible with the legitimate use and flow of data and information in a free society," states the Democracy Principle.

At its best, OECD policy-making can be an exhilarating process. Countries strive to find the common ground that will promote economic growth and respect national differences all the while recognizing that political liberty is an essential precondition for international policy. It is conceivable that such a process could be made to work for some of the hard problems facing the growing Internet community — intellectual property, content regulation.

IT IS AN EXTRAORDINARY SCENE, AS IF US TRADE OFFICIALS AND COMMERCE DEPARTMENT EXPERTS HAD BEEN MUGGED IN THEIR HOTEL ROOMS AND REPLACED BY AGENTS OF A DIFFERENT GOVERNMENT.

But the encryption policy has been unlike previous OECD efforts. The slow, deliberate consensus building effort that produced good polices on security and privacy has been pushed aside in favor of a fast-track strategy recommended by Washington. Government agencies responsible for trade and economic development were asked to step aside for law enforcement officials. The delegation from the United States to the economic organization is chaired not by a member of the Department of Commerce but by the head of the Justice Department's Computer Crime Unit. The NSA rep is close at hand. The former NSA general counsel records the minutes of the meetings for the benefit of his business clients and the US delegation. It is an extraordinary scene, as if trade officials and Commerce Department experts had been mugged in their hotel rooms and replaced by agents of a different government. The DOJ has even managed to place one of its own at the OECD to assist the organization in writing the guidelines in the shortened time-frame.

While early attempts by the US to spin off a secret drafting party ultimately failed, the US delegation — that is to say representatives of the Department of Justice and the National Security Agency and a few business representatives who stand to gain big if key escrow is adopted — succeeded in clouding two critical

issues. Consider, for example, the concept of Trusted Third Parties, which are more frequently called Certification Authorities. For the Europeans, this term typically means digital notaries that could help promote on-line commerce. (My own preference, as I've argued elsewhere, is for anonymous payment schemes that minimize privacy and security risks)

The US said, "why not join your authentication function with our key escrow function?" Now certification authorities, already facing undetermined civil liability, are expected to function also as wiretap clearinghouses. Under the European approach, it may be possible to force such an outcome but the desirability is far from clear. Merging escrow and authentication opens the door to new forms of fraud and criminal conduct. And the liability problems skyrocket.

In another sleight of hand replaying the Clipper debate in the US, the Administration argued that key escrow intended to assist law enforcement could serve business concerns about key management and disgruntled employees. Of course, most organizations would much rather manage their own file recovery procedures and no organization is likely to go for the real-time interception capability that is at the heart of the key escrow plan.

Washington has played its hand well, except for one problem: key escrow makes no sense for the OECD. When Japan, for example, said at one of the early sessions that it could not back the plan for both economic and legal reasons, it simply acknowledged what other countries already knew: a plan developed by the US intelligence agencies to monitor communications in OECD member countries based on US technical standards was about as far down the wish list as any self-respecting delegate to the OECD could imagine.

"YOUR GOVERNMENT HAS TAKEN A RATHER NARROW VIEW OF THE ENCRYPTION ISSUE," A EUROPEAN DELEGATE SAID TO ME DURING ONE OF THE BREAKS BETWEEN SESSIONS IN WASHINGTON.

Since the early sessions, the number of countries that have voiced opposition to the US key escrow proposal has grown. From Canada and Australia to Denmark, Germany, Turkey, Austria, Sweden, the Netherlands, and others, the objections are mounting. Just prior to the last session in Paris, there was even discussion of whether the entire effort should be scrapped. Understandably, the OECD would like something to show for its efforts. but the rumblings about "the US plan" are so great that any policy adopted at this point is unlikely to be more than a diplomatic accommodation. Washington stands increasingly alone.

The arguments against key escrow are many: Several countries have said that requiring users to escrow keys will violate civil liberties and human rights principles. "We must never forget that governments have a responsibility to protect the privacy interests of their citizens," one delegate reminded the gathering in Canberra.

Others have questioned whether it is appropriate for an organization committed to economic development to pursue a policy clearly intended to satisfy law enforcement concerns. "Your government has taken a rather narrow view of the encryption issue," a European delegate said to me during one of the breaks between sessions in Washington.

Still others ask whether it is appropriate that such policies be developed without further input from the public. It is, after all, users who will shape the market for crypto products.

And then there is the critical question of the impact of these policies on recently established democratic governments in Eastern Europe. One advisor to several Eastern European governments who is helping to provide Internet connectivity reminded me that it was proposals such as these that led to the collapse of the Communist governments.

Not surprisingly, the US and business lobbyists who stand to profit from adoption of key escrow have lobbied OECD delegates in between sessions to build support. It is hard to know what's been said in these closed door sessions, but there can be little doubt that many of the tactics developed during the Clipper debate in the US are now being replayed in briefing

sessions around the globe.

Whither Washington?

It is always hard to predict where the OECD countries will come down, but a quick survey suggests that key escrow has a long road ahead. The new government of Australia came into power in clear opposition to escrow encryption. Canada has always placed a premium on international human rights. Denmark's IT panel rejected key escrow. Germany must assess whether the key escrow plan favored by law enforcement outweighs the lost commercial opportunity of robust crypto exports. The Netherlands' delegate has spoken in opposition to the plan. New Zealand is likely to follow Australia's lead. Sweden is holding ranks with its Scandinavian neighbors. Turkey must decide if it will acede to technologies that will do little to promote economic growth. Even France, which clearly wants to maintain domestic surveillance capabilities, must consider if key sharing with foreign intelligence agencies is in its national interests.

Countries are well aware that encryption will pose new challenges to law enforcement. But it is becoming equally clear, as the US National Research Council concluded in a report earlier this year, that one of the best ways to prevent on-line crime and to protect public safety will be to promote the availability of strong encryption.

Indeed, the Japanese position, like the position of many OECD members, is not hard to understand. For the member nations of the OECD, encryption policy is first and foremost about the development of the technical infrastructure for secure on-line transactions to promote economic growth. To the extent that law enforcement concerns enter into the picture, they must be balanced by competing economic and civil liberty interests.

Washington Comes Home

Central to the current OECD debate about encryption policy is the interplay of two principles. The first — Free Choice — states that users and businesses should be free to use whatever form of encryption they wish without government restriction. The second — Government Access — has been described as establishing a government right to access encoded communication.

How are these principles to be reconciled? One approach would be to allow "free choice" within the narrow set of key escrow options. Such an approach is favored by some law enforcement officials but seems unlikely to sway most OECD members or US business.

The better answer for the OECD would be to leave the Free Choice principle in place as the cornerstone of international crypto policy and to treat Government Access principle not as a right to intercept but as an obligation for governments to comply with lawful process when interception occurs without imposing draconian key escrow systems. Such an approach would strengthen the hand of independent judiciaries, promote government accountability, and reaffirm the principle of private communication set out in the Universal Declaration of Human Rights.

AS THE US NATIONAL RESEARCH COUNCIL CONCLUDED IN A REPORT EARLIER THIS YEAR, THAT ONE OF THE BEST WAYS TO PREVENT ON-LINE CRIME AND TO PROTECT PUBLIC SAFETY WILL BE TO PROMOTE THE AVAILABILITY OF STRONG ENCRYPTION.

For governments in Eastern Europe and others struggling to build democratic institutions, it would also send a clear message that principles of liberty must place constraints on the government before the governed. And, consistent with the mission of the OECD, it would replace wartime policies with those intended to promote economic growth and international cooperation.

The traditions of the OECD weigh in favor of such an outcome. Indeed, the traditions of the United States would argue for this result as well.

Marc Rotenberg is director of the Electronic Privacy Information Center (http://www.epic.org). He served on the OECD expert panel on information security and currently advises the OECD Secretariat on encryption policy.

TWELVE ARGUMENTS AGAINST ID CARDS

Proposals for national ID cards are causing debate across the world. In this article, Privacy International discusses the key arguments against such cards.

1. They Do Not Stop Crime

Law and order is the main motivation behind current efforts to introduce an ID card in the UK. Home Secretary Michael Howard told the 1994 Tory Party conference that he believed an ID card could provide an invaluable tool in the fight against crime.

Howard's claim has received little support from academic or law enforcement bodies. The Association of Chief Police Officers (ACPO) said that while it is in favor of a voluntary system, its members would be reluctant to administer a compulsory card that might erode relations with the public. Dutch police authorities were not generally in favor of similar proposals in that country, for much the same reason.

POLICE AND CRIMINOLOGISTS HAVE NOT BEEN ABLE TO ADVANCE ANY EVIDENCE WHATEVER THAT THE EXISTENCE OF A CARD WOULD ACTUALLY REDUCE THE INCIDENCE OF CRIME.

According to police in both countries, the major problem in combating crime is not lack of identification procedures, but difficulties in the gathering of evidence and the pursuit of a prosecution. Indeed, police and criminologists have not been able to advance any evidence whatever that the existence of a card would actually reduce the incidence of crime. In a 1993 report, ACPO suggested that street crime, burglaries, and crimes by bogus officials could be diminished through the use of an ID card, though this conflicted with its position that the card should be voluntary.

In reality, it appears that only a national DNA database (such as the one recently opened in Britain) or a biometric database (such as the one proposed in Ontario) might assist the police in linking crimes to perpetrators.

There is a powerful retributive thread running along the law and order argument. Some people are frustrated by what they see as the failure of the justice system to deal with offenders, and the ID card is seen, at the very least, as having an irritant value.

2. They Do Not Stop Welfare Fraud

Benefits agencies around the world have identified problems relating to fraud. Three levels of fraud are often expressed, in order of significance, as (1) false declaration, or non-declaration, of income, (2) Criminal acquisition of multiple benefits using false identification, and (3) More conventional fraud and theft of benefit payments.

There also exist numerous other factors which contribute to benefit overpayment, including clerical error and genuine misunderstanding about the terms of payment.

No-one knows the true extent of fraud. Virtually no ethnographic research exists, and the data that do exist are drawn principally from internal and external audits, management reviews, and retrospective studies. Many studies assess risk, rather than quantifying fraud. Estimates of the extent of fraud on benefits agencies vary to a far greater extent than do the conditions in each recipient population.

The Parliamentary Select Committee on the Australia Card warned that the revenue promises were little better than a "Qualitative assessment" - in other words, guesswork. The Department of Finance refused to support the Health Insurance Commission's cost benefit estimates. Revenue was constantly revised downward, while the costs continued to rise. The Department of Social Security insisted that the ID card would have done little or nothing to diminish welfare

fraud. In evidence to the parliamentary committee investigating the proposal, the Department said that much less than one percent of benefit overpayments resulted from false identity. The Department decided that it would pursue other means of tackling fraud. The DSS in the UK argued against ID cards on the same grounds.

The Australian DSS estimates that benefit overpayment by way of false identity accounts for 0.6 per cent of overpayments, whereas non-reporting of income variation accounts for 61 per cent. The key area of interest, from the perspective of benefit agencies, lies in creating a single numbering system which would be used as a basis for employment eligibility, and which would reduce the size of the black market economy.

3. They Will Not Stop Illegal Immigration

The immigration issue appears to be the principal motivation behind ID card proposals in continental Europe, the United States and many developing nations.

The abolition of internal borders has become a primary concern of the new European Union. The development of the Schengen agreement between the Benelux countries, France and Germany calls for the dismantling of all border checks, in return for a strengthening of internal procedures for vetting of the population. France and the Netherlands have already passed legislation allowing for identity checks on a much broader basis, and other countries are likely to follow.

The establishment of personal identity in the new borderless Europe is a contentious issue, but is one which appears (to many people) to be a broadly acceptable trade-off for the convenience of total freedom of movement within the union.

The use of a card for purposes of checking resident status depends on the police and other officials being given very broad powers to check identity. More important from the perspective of civil rights, its success will depend on the exercise of one of two processes: either a vastly increased level of constant checking of the entire population, or, a discriminatory checking procedure which will target minorities.

The two arguments most often put forward to justify the quest to catch illegal immigrants in any country are (1) that these people are taking jobs that should belong to citizens and permanent residents, and (2) that these people are often illegally collecting unemployment and other government benefits.

The image of the illegal immigrant living off the welfare of the State is a powerful one, and it is used to maximum effect by proponents of ID cards. When the evidence is weighed scientifically, it does not bear any resemblance to the claim. When the Joint Parliamentary Committee on the Australia Card considered the issue, it found that the real extent of illegal immigrants collecting government benefits was extremely low. The report described a mass data matching episode to determine the exact number. Of more than 57,000 overstayers in New South Wales, only 22 were found in the match against Social Security files to be receiving government unemployment benefits. That is, 22 out of a state population of five million. The Department of Immigration and Ethnic Affairs (DIEA) had earlier claimed that the figure was thirty times this amount (12.4 per cent as opposed to 0.4 per cent of overstayers).

THERE IS A POWERFUL RETRIBUTIVE THREAD RUNNING ALONG THE LAW AND ORDER ARGUMENT. SOME PEOPLE ARE FRUSTRATED BY WHAT THEY SEE AS THE FAILURE OF THE JUSTICE SYSTEM TO DEAL WITH OFFENDERS, AND THE ID CARD IS SEEN, AT THE VERY LEAST, AS HAVING AN IRRITANT VALUE.

Once again, immigration authorities worldwide base their estimates on qualitative assessment or, to put it more bluntly, guesswork. Again quoting from the Australia Card inquiry, "It became clear that the estimates for illegal immigrants were based on guesswork, the percentage of illegal immigrants who worked was based on guesswork, the percentage of visitors who worked illegally came from a Departmental report that was based on guesswork....The Committee

has little difficulty in rejecting DIEA evidence as being grossly exaggerated."

4. They Facilitate Discrimination

As mentioned earlier in this section, the success of ID cards as a means of fighting crime or illegal immigration will depend on the exercise of one of two processes: either a vastly increased level of constant checking of the entire population, or, a discriminatory checking procedure which will target minorities.

DISCRIMINATORY PRACTICES ARE AN INHERENT PART OF THE FUNCTION OF AN ID CARD. WITHOUT THIS DISCRIMINATION, POLICE WOULD BE REQUIRED TO CONDUCT RANDOM CHECKS, WHICH IN TURN, WOULD BE POLITICALLY UNACCEPTABLE.

The irony of the ID card option is that it invites discrimination by definition. Discriminatory practices are an inherent part of the function of an ID card. Without this discrimination, police would be required to conduct random checks, which in turn, would be politically unacceptable.

All discrimination is based on one of two conditions: situational or sectorial. Situational discrimination targets people in unusual circumstances. i.e. walking at night, visiting certain areas, attending certain functions or activities, or behaving in an abnormal fashion. Sectorial discrimination targets people having certain characteristics, i.e. blacks, youths, skinheads, motor cycle riders or the homeless. ID cards containing religious or ethnic information make it possible to carry this discrimination a step further.

Several developed nations have been accused of conducting discriminatory practices using ID cards. The Government of Japan recently came under fire from the United Nations Human Rights Committee for this practice. The Committee had expressed concern that Japan had passed a law requiring that foreign resideuts must carry identification cards at all times.

French police have been accused of overzealous use of the ID card against blacks, and particularly against Algerians. Greek authorities have been accused of using data on religious affiliation on its national card to discriminate against people who are not Greek Orthodox. ID checks by Belgian police sparked race riots in the early 1990s. During the campaign against the Australia card, aboriginals and Jewish leaders expressed fear of discrimination, while in New Zealand, trades unions and civil liberties organizations warned of discrimination against minority groups and poor people.

5. They Invariably Create an Unwarranted Increase in Police Powers

The Privacy International survey of ID cards found claims of police abuse by way of the cards in virtually all countries. Most involved people being arbitrarily detained after failure to produce their card. Others involved beatings of juveniles or minorities. There were even instances of wholesale discrimination on the basis of data set out on the cards.

While it is true that cards containing non-sensitive data are less likely to be used against the individual, cards are often alleged to be the vehicle for discriminatory practices. Police who are given powers to demand ID invariably have consequent powers to detain people who do not have the card, or who cannot prove their identity. Even in such advanced countries as Germany, the power to hold such people for up to 24 hours is enshrined in law. The question of who is targeted for ID checks is left largely to the discretion of police.

The wartime ID card used in the UK outlived the war, and found its way into general use until the early 1950s. Police became used to the idea of routinely demanding the card, until in 1953, the High Court ruled that the practice was unlawful. In a landmark ruling that led to the repealing of the National Registration Act, and the abandonment of the ID card, the Lord Chief Justice remarked :

> although the police may have powers, it does not follow that they should exercise them on all occasions...it is obvious that the police now, as a matter of routine,

> demand the production of national registration identity cards whenever they stop or interrogate a motorist for any cause....This Act was passed for security purposes and not for the purposes for which, apparently it is now sought to be used.... in this country we have always prided ourselves on the good feeling that exists between the police and the public, and such action tends to make the public resentful of the acts of police and inclines them to obstruct them rather than assist them.

6. They Tend to Become an Internal Passport

Virtually all ID cards worldwide develop a broader usage over time, than was originally envisioned for them. This development of new and unintended purposes has become known as function creep.

All compulsory ID cards - and even the majority of non-compulsory ones - develop into an internal passport of sorts. Without care, the card becomes an icon. Its use is enforced through mindless regulation or policy, disregarding other means of identification, and in the process causing significant problems for those who are without the card. The card becomes more important than the individual.

In most countries with a card, its use has become universal. All government benefits, dealings with financial institutions, securing employment or rental accommodation, renting cars or equipment and obtaining documents requires the card. It is also used in myriad small ways, such as entry to official buildings (where security will invariably confiscate and hold the card).

Ironically, many card subjects come to interpret this state of affairs in a contra view (the card helps streamline my dealings with authority, rather than the card is my licence to deal with authorities). The Australia Card campaign referred to the card as a licence to live.

7. A Voluntary Card Always Becomes Compulsory

Any official ID system will ultimately extend into more and more functions. Any claim that an official card is voluntary should not imply that a card will be any less of an internal passport than would a compulsory card. Indeed a voluntary card may suffer the shortcoming of limited protections in law. Comments by correspondents in many countries suggests that even where a card is voluntary it is so inconvenient not to have one that they are effectively compulsory.

During the campaign against the Australia Card, talk back radio hosts had become fond of quoting a paragraph of an HIC planning document on the Australia Card:

> It will be important to minimize any adverse public reaction to implementation of the system. One possibility would be to use a staged approach for implementation, whereby only less sensitive data are held in the system initially with the facility to input additional data at a later stage when public acceptance may be forthcoming more readily.

8. The Cost is Usually Extremely High

In the Philippines and Australia, the cost of implementing an ID system has been at the forefront of opposition. The Philippines proposal relied on government estimates that were drawn, as is often the case, from estimates calculated by computer industry consultants. These were found to under-estimate the true cost by eight billion pesos over seven years. The proposal lapsed because of this factor.

ALL COMPULSORY ID CARDS - AND EVEN THE MAJORITY OF NON-COMPULSORY ONES - DEVELOP INTO AN INTERNAL PASSPORT OF SORTS.

In Australia, the cost of the proposed ID card failed to take into account such factors as training costs, administrative supervision, staff turnover, holiday and sick leave, compliance costs, and overseas issue of cards. Other costs that are seldom factored into the final figure (as was the case in Australia) are the cost of fraud, an underestimate of the cost of issuing and maintaining cards, and the cost to the private sector.

As a consequence, the official figure for the Australia card almost doubled between 1986 and 1987.

Private sector costs for complying with an ID card are very high. The Australian Bankers Association estimated that the system would cost their members more than one hundred million dollars over ten years. Total private sector compliance costs were estimated at around one billion dollars annually.

The official figure for the Australia card was $820 million over seven years. The revised estimate including private sector and compliance costs, together with other factors, would amount to several times as much.

PEOPLE WHO LOSE A WALLET FULL OF CARDS QUICKLY UNDERSTAND THE MISFORTUNE AND INCONVENIENCE THAT CAN RESULT. A SINGLE ID CARD WHEN LOST OR STOLEN CAN HAVE AN EVEN GREATER IMPACT ON A PERSON'S LIFE.

The UK Government's CCTA (Information Technology Center) advised that a national smart ID card would cost between £5 and £8 per head, yet this figure does not include administration or compliance. The cost of a card system could ultimately be as high as £2 billion or £3 billion.

9. The Loss of a Card Always Causes Great Distress and Inconvenience

Virtually all countries with ID cards report that their loss or damage causes immense problems for people. Up to five per cent of cards are lost, stolen or damaged each year, and the result can be denial of service ad benefits, and - in the broadest sense - loss of identity.

There exists a paradox in the replacement of cards. The replacement of a high security, high integrity card involves significant administrative involvement. Documents must be presented in person to an official. Cards must be processed centrally. This process can take some weeks. A low value card can be replaced more quickly, but its loss poses security threats because of the risk of the potential for misuse.

People who lose a wallet full of cards quickly understand the misfortune and inconvenience that can result. A single ID card when lost or stolen can have an even greater impact on a person's life.

10. A Card Imperils the Privacy of Personal Information

The existence of a person's life-story in a hundred unrelated databases is one important condition that protects privacy. The bringing together of these separate information centers creates a major privacy vulnerability. Any multi-purpose national ID card has such an effect.

Privacy advocates argue against ID cards on the basis of evidence from various security threat models in use throughout the private sector. In these models, it is generally assumed that at any one time, one per cent of staff will be willing to sell or trade confidential information for personal gain. In many European countries, up to one per cent of bank staff are dismissed each year, often because of their involvement in theft.

The evidence for this potential corruption is compelling. Recent inquiries in Australia, Canada, and the United States indicate that widespread abuse of computerised information is occurring. Corruption among information users inside and outside the government in New South Wales had become endemic and epidemic. Virtually all instances of privacy violation related to computer records.

A UK National Audit Office (NAO) report from March 1995 revealed that computer hacking, theft and viruses are on the rise in Whitehall's developing IT network. Instances of hacking rose by 140 percent in 1984, while viruses increased by 300 percent. 655 cases of hacking were identified by the NAO. Most of these involved staff exceeding their authority by obtaining information on members of the public to disclose to non-authorized people.

11. Card Systems Entrench Criminality and Institutionalize False Identity

Remarkably, the main problem for all ID card

systems, is not the inevitable conflict with civil rights. It is the curious repercussion that a card actually entrenches crime. By providing a one stop form of identity, criminals can easily use cards in several identities. Even the highest integrity bank cards are available as blanks in such countries as Singapore for several dollars. Within two months of the new Commonwealth Bank high security hologram cards being issued in Australia, near perfect forgeries were already in circulation.

This argument has been advanced in Australia, the UK, and the Netherlands. It relies on the simple logic that the higher an ID card's value, the more it will be used. The more an ID card is used, the greater the value placed on it, and consequently, the higher is its value to criminal elements. Organizations come to rely on the card as an unquestioned proof of ID, and often abandon the checking systems that have evolved over many years.

12. They Compromise National Identity and Personal Integrity

ID cards strike a nerve in the national psyche of some countries. ID cards are often viewed as inimical to the struggle for independence, freedom, autonomy and individuality that nations cherish. The Australia Card campaign vividly illustrates this phenomenon.

Privacy protection involves resistance to the establishment or consolidation of monolithic information systems. Informational chaos among agencies has ensured that the individual has not become a servant to the state. Variety, choice, and chaos have also had the effect of ensuring the free movement, rights, and free choice of individuals.

The movements against ID cards in the US, Canada, Australia, and New Zealand have highlighted a number of abstract fears, widely held throughout the population, such as:

- people will be de-humanised by being reduced to numbers;
- the system is a hostile symbol of authority;
- society is becoming driven by technology driven bureaucracy, rather than by elected government;
- such identification schemes are the mechanism foretold in religious prophecy (e.g. 'the Mark of the Beast').

While these fears may be dismissed by proponents of ID card, they ultimately will be the fuel for public disquiet.

Conclusion

Generally speaking, the key element of any modern ID card is the number. The number is the common element within all databases, and is the key to access all this personal information. With this number, governments can establish computer linking programs that merge information on many aspects of a person's life.

Privacy International has set up an extensive web page on national ID cards including a 7,000 word Frequently Asked Questions (FAQ) report, a summary of views from around the world, an analysis of successful campaigns, and other materials or current proposals in the UK and from around the world. The web page address is: http://www.privacy.org/pi/activities/idcard/

Biometrics - Continued from Page 1

information systems security in recent years has been to create ways of establishing accurate identity without the trappings of Big Brotherism.

Biometrics

There are three conventional forms of identification 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 number. The third is something you "*are*" or something you "*do*" , such as a fingerprint, handwriting, or voice print. This latter form of identification is known as "biometrics".

AN OVERLY RIGOROUS IDENTIFICATION PROCEDURE COULD PROVE UNPOPULAR, FORCING SOME PEOPLE TO DROP OUT OF THE SYSTEM, AND INVITING A DEGREE OF CIVIL DISOBEDIENCE IN OTHERS.

The most popular forms of biometric ID are retina scans, hand geometry, thumb scans, finger prints, voice recognition, and digitized (electronically stored) photographs. While some forms of biometic identification, such as fingerprints, have existed for nearly a century, scanning, networking and searching technologies have now automated the processes.

Biometric technology offers the prospect of highly accurate identification, but involves some difficult technical and public relations problems. In western nations, the use of fingerprinting invites the stigma of criminality. Technical difficulties also dominate the use of sophisticated identification technology. Many systems do not live up to expectations because they fail to take into account the needs of people, or because the manufacturers provide inadequate testing under sterile conditions.

Flawed identity checking is very costly for organizations. It results in unnecessary duplication, fraud, and client disruption. A high integrity universal biometric system would, from the perspective of information users, be an ideal solution. Yet, from the perspective of privacy and autonomy, the move to such a universal form of identity carries enormous risks. There is a possibility of "statelessness" arising where the system requires an increasing level of compliance which some people simply cannot or will not accept, thus, they end up being denied a range of services. Errors or failure in one part of the system may lead to a domino effect involving suspension of benefits or entitlements in other areas. Most importantly, the autonomy and freedom of individuals may be compromised because of the scale and nature of information collection.

Although biometry is increasingly seen as a solution to fraud and inefficiency, not everyone is happy with the technology. Daniel Polsby, a law professor at the Northwestern University in the US warns that a loss of personal privacy will be the price. "If the technology becomes as efficient and cheap as expected, it almost certainly will be widely used. The possibilities of abuse are mind-boggling," Polsby says. "With this technology, the government can compile a dossier on a person that tracks his every purchase and movement. That sort of thing is possible now, but it is too labor-intensive and expensive."[4]

In recent years, biometric technology has attained a remarkable level of sophistication, and reported 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 from 10 to the 15th power on the first scan, and from 10 to the 22nd power on the second scan. In other words, the chances of the match being incorrect are one in fifteen thousand trillion.[6] The figure may be off by a vast amount, but the accuracy of the procedure is still without parallel in the field of identification. Iris recognition does suffer from the shortcoming that many people feel very sensitive and protective of their eyes, and find such technology unsettling. 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. The Biometric Technologies Company

of the US is in the final stages of developing a biometric fingerprinting system using neural networks. Laboratory tests commissioned by the manufacturer are showing an accuracy of 99.99 percent, and a false rejection rate (rejecting genuine clients) of 0.1 percent Known as Printscan 3, the device is expected to cost US$600 per unit.[7]

The Japanese Telecommunications giant NTT recently announced the development of a fingerprint recognition method that appears to be exceptionally fast and accurate. The technique can be used in conjunction with ordinary information processing and communications systems. Recognition of a fingerprint takes place in an average of two seconds on a personal computer or one second on a workstation, with accuracy above 99.9 percent. Along with many other diverse applications, it can be used to confirm that the bearer of a credit card or ID card is the rightful owner. National computerised fingerprint systems are now being developed in several countries. The first national system was developed in Australia in 1987 using Fujitsu technology.[8]

The development of hand geometry, involving a scan of the shape and characteristics of the entire hand, has been an alternative approach in situations where there is public sensitivity to fingerprinting. Hand geometry is already employed in over 4,000 locations in the US and Europe, including airports, day care centers, nuclear research establishments, computer facilities, sperm banks, hospitals and in high security government buildings. [9]

An automated immigration system developed by the United States Immigration and Naturalization Service (INS) uses hand geometry (see below). In this project, frequent travellers to the United States have their hand geometry stored in a "smart" computer chip card. The traveller places a hand onto a scanner, and places the card into a slot. However, a similar project which was to commence shortly in Germany apparently rejected the hand geometry system because of inaccuracies in the technology. The problem demonstrates the extent to which controlled laboratory trials are of limited value in the real world.[12]

This system has the potential to pioneer a worldwide biometric system. It is feasible that within fifteen years, all countries will introduce such systems, and share this information. Some experts believe that by 2010, all travellers to and from the United States will need to be biometrically registered. Information about passengers will be shared on the basis of the biometry.

Countries around the world are jumping on the bandwagon. Spain is planning a national fingerprint system for unemployment benefit and healthcare entitlement. Russia has announced plans for a national electronic fingerprint system for banks. In the near future, Jamaicans will need to scan their thumbs into a database before qualifying to vote at elections. In the US, Blue Cross and Blue Shield have plans to introduce nationwide fingerprinting for hospital patients. This may be extended into more general medical applications. In Europe, tests are under way with equipment that puts a person's fingerprint information onto his or her credit card so a device at the point of purchase can compare the card's data to a fingerprint to assure that the use of the card is legitimate. In Australia, the technology is being used in retail outlets, government agencies, prisons, police forces and automated-teller machines. As it becomes more viable, biometric technology is likely to be adopted as the identification of choice for large, complex organizations.

"WITH THIS TECHNOLOGY, THE GOVERNMENT CAN COMPILE A DOSSIER ON A PERSON THAT TRACKS HIS EVERY PURCHASE AND MOVEMENT. THAT SORT OF THING IS POSSIBLE NOW, BUT IT IS TOO LABOR-INTENSIVE AND EXPENSIVE."

DANIEL POLSBY
NORTHWESTERN UNIVERSITY

Giving Welfare a Hand in the UK

In January 1994, senior officials of the UK Department of Social Security met with their chief, Peter Lilley to discuss ways of reducing welfare fraud,

which is estimated to cost more than £2 billion annually. The DSS recommended a number of options. Surprisingly, the Department ended up supporting an initiative potentially far more controversial than the ID card which was on the drawing board. Its favored option was to create a computerised database of the hand prints of every person receiving a government benefit. These would be stored in digitized form in a central computer. Whenever a person applied to a government agency for a benefit or subsidy, a hand print would be taken to determine whether that person already existed in "the system". The Department estimated that as many as thirty million people would have to be "palm printed".

SOME EXPERTS BELIEVE THAT BY 2010, ALL TRAVELLERS TO AND FROM THE UNITED STATES WILL NEED TO BE BIOMETRICALLY REGISTERED. INFORMATION ABOUT PASSENGERS WILL BE SHARED ON THE BASIS OF THE BIOMETRY.

The Department's reasons for recommending this strategy are largely to do with its ramshackle administration, a woe which it shares with many other agencies. Identification procedures are haphazard. Many clients simply do not have the necessary ID documents. While the problem of false or multiple identities is generally overstated, it nevertheless remains a political and administrative nuisance.

Fingerprinting the Populace in Canada

The provincial government of Ontario in Canada is considering a biometric scheme which it hopes will eliminate fraud and duplication, and streamline the functioning of all government agencies. The *Client Positive Identification Strategy* has been pioneered by the Community Services Department of Metro Toronto, an agency which hands out around two billion Dollars Canadian (£1 billion) per annum on welfare services. The Department is steering a government wide exploration of a biometric system which may eventually be used for all government benefits and services.

A committee representing virtually all Ontario Departments has been established. It is currently discussing the mutual identification and administration concerns, and the potential for creating a universal strategy for dealing with these problems.[13] Although planning is still in the preliminary stage, officials are hopeful that a biometric register of thumb scans can be established by 1996. The register would be accessed by all Ontario agencies, and scanners (readers) would be located at many "convenient" locations. The idea is to create a "once and for all" identity which would then be valid for all government services and benefits. Discussions are underway with Federal agencies to see whether this program can be integrated with immigration systems.

The motivation behind this interface is that there is currently great concern over the issue of US citizens illegally using Canadian health care facilities. Ironically, US authorities have criticized Canadians for crossing the border to use the "superior" American health system. The specifications set out in government documents describe a system that will digitize and store photographs and hand geometry, interface with existing information systems, and produce a plastic identity card with magnetic stripe.

The Project Manager for the strategy believes that the plan is technologically and organizationally possible, but "politically tricky". The Privacy Commissioner for Ontario has expressed grave reservations, but his involvement to this point has been minimal. It appear that the departments are compiling as much data as possible on the topic before formally presenting the plan to Cabinet.

A Hand Across the Border

In 1993, the US immigration authorities opened a intriguing new immigration lane in New York's John F. Kennedy airport. What distinguished it from the traditional immigration procedure was that this new lane was entirely controlled by computer technology. Remarkably, it could automatically identify and process a passenger in as little as twenty seconds.

Known as FAST (Future Automated Screening

for Travellers), the lane identifies passengers from the characteristics of their hand, rather than from their passport and photograph. It then connects with the standard immigration computer systems to determine the passenger's status.

These automated immigration lanes are appearing throughout the world - in Toronto, Frankfurt, Amsterdam, and on the US-Mexico border - as part of an international experiment intended to revolutionize the world's immigration systems.

The project, called INSPASS (Immigration and Neutralization Service Passenger Accelerated Service System), has for the past fourteen months been operating as a voluntary system for frequent travellers. More than 65,000 people have so far enrolled in the system, a figure which increases by almost 1,000 a week. Governments in 26 countries - including the UK - are coordinating with the project.

If the INSPASS trial is successful, the technology may ultimately make conventional ID cards and passports redundant. And, as a trade-off for faster immigration processing, passengers will have to accept a system which has the potential to generate a vast amount of international traffic in their personal data. Ultimately, a universal immigration control system may be linked to a limitless spectrum of information, such as police and tax systems.

An in-house evaluation of the system has given INSPASS the green light. INS officials are now confident that a universal project can be established, using common international standards and a smart card system that can cope with either a hand geometry or a fingerprint scan. According to staff working with the INSPASS project, all European governments are committed to the goal of automated immigration processing.

The thorny question is whether such a system might ultimately be manipulated by governments and airline companies anxious to receive more information about passengers.

Future Imperfect ?

To date only limited testing of biometrics has been carried out by independent agencies. Best known

How INSPASS Works

INSPASS is available to frequent travellers to and from the US, who are US or Canadian Nationals, or Nationals of the 32 countries involved in the US visa waiver scheme. The countries participating in the trial are Andorra, Austria, Belgium, Bermuda, Canada, Denmark, Finland, France, Germany, Iceland, Italy, Japan, Liechtenstein, Luxembourg, Monaco, The Netherlands, New Zealand, Norway, San Marino, Spain, Sweden, Switzerland and the United Kingdom. Travellers who visit the United States at least three times a year are "invited" to apply in writing for INSPASS registration. Applicants then attend one of the INSPASS enrollment centres at JFK or Newark airports, where they are interviewed, and their identity confirmed.

This completed, the traveller places the palm of a hand onto the surface of a scanner, which then records intricate measurements and details of the hand's shape and contours. These are converted into a "template" and stored on a card (currently a paper card, but soon to be a smart card). Fingerprints are also taken and recorded at this point.

Whenever INSPASS members enter the two test airports, they bypass the main immigration queues, and go straight to the INSPASS "Kiosk". Once inside, the card is presented to the terminal, which confirms its' status. The hand is then placed onto a scanner. This matches the biometry of the palm with the "template" encoded into the card. The Immigration Information systems 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.

An increasing number of countries are already subscribing to a "Blue Lane" information exchange system in which passenger information is transmitted in advance of the journey.

is the work of the US Department of Energy's Sandia National Labs, which released the results of its second round of tests on biometric devices in mid-1990. Encouraging as they are, these tests have to be questioned, since they assessed equipment from only six US vendors out of several dozen in the marketplace. Hardly a truly representative sample of internationally available biometric products.[14]

Nonetheless, these tests are currently the only comprehensive evaluations available. They showed that dynamic signature verification (DSV) is by far the cheapest of the evaluated product types, although these latest tests also reveal that DSV rejects a disturbingly 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 - but it costs more than twice as much. The poorest performer was voice verification, exhibiting very high false rejection rates and a relatively high false acceptance rate. Voice verification systems have been implemented by a number of financial institutions in association with the introduction of telephone banking services. Voice-based services are clearly seen by the banks to be the most immediately rewarding area of biometric systems,[15] but the higher accuracy of other biometric systems will ultimately make them the identification systems of choice for government and private sector alike.

THE EXPERIENCE INTERNATIONALLY IS THAT ATTEMPTS TO RESOLVE INEFFICIENCIES IN THE HEALTH, POLICE OR SOCIAL SECURITY SECTORS OFTEN RESULTS IN NEW UNFORSEEN PROBLEMS AND COSTS.

A Disaster Waiting to Happen

The benefits of large-scale computerization are erratic, unpredictable, and usually less satisfying than expected. No vendor or systems designer can predict with certainty the extent to which a system will succeed or fail. Computer failures compound disproportionately to the size and complexity of the system While there are numerous examples where information systems within particular areas of government can deliver savings and additional benefits to clients and users, the case for multi-faceted integration of complex systems (i.e. the creation of a nationwide integrated biometric and administrative system) is less convincing.

The computer system for the Europe-wide Schengen police information sharing system has been constantly paralysed because of unforeseen human and technical problems. The FBI and the UK national police electronic fingerprinting systems have also suffered. Where computer systems fail to deliver expected performance or returns, it is invariably clients and customers who suffer.

The warnings were ever present. In 1995, the UK police automated national fingerprint system was shut down because the technical specifications did not match the organizational requirements of the police. A nasty legal battle ensued between the police and the supplier, IBM.

It is true, of course, that government service delivery is often inefficient. It is equally true that the relevant information is fragmented and inconsistent. However, it does not follow that a centralized plan of action can resolve the many factors that contributed to these circumstances. In a perfect world, shortcomings can be identified and solutions implemented with equal effectiveness. The experience internationally is that attempts to resolve inefficiencies in the health, police or Social Security sectors often results in new unforseen problems and costs.

A 1993 report commissioned by the United States Department of Health and Human Services noted that there existed a vast gulf between the promise and the reality of savings from computer systems.[16] A study by the Congressional Office of Technology Assessment found that computer based information systems, once implemented, often result in "unforseen costs, unfulfilled promises, and disillusionment".[17]

The pursuit of perfect identification involves a number of important technological, organizational,

social, legal, and political issues. Modern identification systems rely on technology that is far from proven. Biometric systems have not been tested on a nationwide basis. They are, to a different and perhaps lesser extent, subject to the same problems that exist at present in more conventional ID schemes.

The administrative and IT systems that form the basis of such ID schemes have been shown in several countries to be much less accurate and cost effective than was originally estimated. Years after the governments of the United States and Australia developed schemes to match public sector computers to save money, there is still no clear evidence that the strategy has succeeded in achieving its original goal. The audit agencies of both federal governments have cast doubt that computer matching schemes deliver savings in many key areas.

There are a great many complexities involved in the introduction of modern identity systems. The integration of computer systems and the merging of information brings with it the need for major organizational restructure. The use of identity procedures also changes the nature of relationships and transactions between clients and departments. Flawed technology has caused grief for organizations that rely on a consistent relationship with their client base. History shows that many organizations are not prepared to take these factors into account.

Any discussion of the risks involved in an integrated ID scheme will intersect considerably with concerns over computerization in general. The vulnerabilities of a computerised biometric system - at a human and organizational level - are very similar to the vulnerabilities of any integrated information system. All modern nationwide ID schemes are part of a larger information strategy. ID cards or biometric templates are used for several purposes, and are the basis of the sharing of data among organizations.

Problems of privacy and confidentiality are perhaps the most important non-budgetary problems created by these proposals. On the one hand, computers offer the promise of creating secure communications through encryption of information. On the other hand, they tend to be a conduit for the distribution of information to a great many locations, and they thus increase the risk of unauthorized access and unforseen use. Systems designers are often fixated by the theme of security, without glancing at the larger picture of how data is collected and distributed.

There exists a number of obvious privacy problems with any system that entails the establishment of a central registry, or even a distributed, but interconnected repository of personal identities. It is uncertain whether the establishment of a repository of identification data would be covered by many data protection laws. A biometric print may be considered in the public domain, or it may find its way into general use by way of implied consent of the individual. In this way, people may find that they are required to provide a biometric print in many unforseen or unintended future circumstances.

Identification systems throughout the world have a history of being ultimately used for unintended purposes. The Social Security number in the US and the Tax File Number, the Dutch SOFI number, and the Austrian Social Security number have been extended progressively to include such facets as unemployment benefits, pensioner benefits, housing entitlement, bank account verification, and higher education. There is a very real possibility that anything as widespread as a general purpose biometric system could mutate. The mere existence of a multi-purpose system of this magnitude will create irresistible opportunities to collect vast amounts of personal information .

MODERN IDENTIFICATION SYSTEMS RELY ON TECHNOLOGY THAT IS FAR FROM PROVEN. BIOMETRIC SYSTEMS HAVE NOT BEEN TESTED ON A NATIONWIDE BASIS. THEY ARE, TO A DIFFERENT AND PERHAPS LESSER EXTENT, SUBJECT TO THE SAME PROBLEMS THAT EXIST AT PRESENT IN MORE CONVENTIONAL ID SCHEMES.

At a society-wide level, the creation of a biometric system involves a number of risks. Privacy advocates

have, traditionally, resisted the establishment of monolithic information systems. Informational chaos and functional separation among agencies have ensured that the individual does not become too closely dependent on the correct functioning of a single system. Variety, choice, and chaos also have the effect of ensuring that the free movement, rights, and free choice of individuals is not compromised by errors in the system.

General purpose biometric systems carry with them two essential dangers. The first is that a problem in identifying a person's hand may affect one's dealings with a range of agencies which use the biometric identifier. This is the same problem that accompanies general purpose ID cards which are lost, stolen or damaged, or which have in some way been "flagged" by the system. The inherent dangers is that while a card carries the presumption of fragility and temporariness, a hand does not. Alternative means of identification may not be built into the system.

VARIETY, CHOICE, AND CHAOS ALSO HAVE THE EFFECT OF ENSURING THAT THE FREE MOVEMENT, RIGHTS, AND FREE CHOICE OF INDIVIDUALS IS NOT COMPROMISED BY ERRORS IN THE SYSTEM.

The second problem involves the less tangible impact on the individual and society. The result may be a real or perceived increase in the power and influence of government administration. Biometrics, more than other ID schemes, may imperil the sense of individuality.

Conclusion

Biometry is, in many senses, a natural extension of this 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. Given the evidence from recent times, it is likely that this awareness is thin on the ground.

---

[1] S.Davies, Big Brother, p.42.

[2] Author's interview with the ATO, January 1996.

[3] ibid.

[4] S.Davies "Touching Big Brother : How biometric technology will fuse flesh and machine", Information Technology and People, MCB University Press, Bradford UK. Vol 7 No 4, 1994 p.43.

[5] Biometric Technology Today, November 1993, Vol 1 Number 7.

[6] ibid p.7.

[7] S.Davies, Touching Big Brother.

[8] Telecommunications Association New Era JapanAugust 15, 1993 NTT Develops Rapid, Highly Accurate Fingerprint Recognition Technique.

[9] Biometric Technology Today (BTT), Vol 1 No. 7, November/December 1993, p. 1.

[10] BTT Vol 2 No. 4, July/August 1994.

[11] Interview with German Federal Data Protection Commissioners Office.

[12] Interview with project Manager, January 19th 1994.

[13] Journal of Electronic Defense, January, 1993 Biometrics futures; EW Design Engineers' Handbook & Manufacturers Directory, Sherman, Robin L.

[14] Ibid.

[15] US Department of Health and Human Services; Workgroup on Computerisation of Patient Records "Toward a national health information infrastructure", report to the Secretary, April 1993 (HHS, 1993).

[16] Office of Technology Assessment (OTA) "Protecting Privacy in Computerised Medical Information" US Government Printing Office, Washington DC, 1993.

Simon Davies is a fellow at the London School of Economics and Director General of Privacy International. This article origionally appeared in his recent book Big Brother (Pan Books, 1996).

PRIVATE PARTS

AN AD-HOC COLUMN OF MISCELLANEOUS ITEMS

Albania

The Albanian Supreme Court on April 23 rejected an appeal by 13 deputies who have been banned from running in the upcoming general elections, Albanian media reported. A commission screening candidates for the elections ruled that they have a communist past. The Supreme Court rejected the deputies' request that they be given access to the documents on which the commission based its decision. It argued that there was enough evidence against them, since their names were included in a file listing those who collaborated with the Sigurimi, the communist-era secret service. Another 26 deputies have also appealed to the court. (Fabian Schmidt, OMRI Inc., April 24, 1996).

Australia

The New South Wales Attorney General announced new privacy legislation on April 4. The Privacy Committee would be merged with the Discrimination board and would be given subpoena powers. Individuals that had their personal information abused by government officials could be compensated up to $40,000 and criminal changes could be brought against the official. The legislation was advanced after it was revealed that a Department of Community Services official had stolen the file of a state ward. (*Australian Associated Press*, April 4, 1996).

Austria

The Austrian government rejected attempts by the European Union to pressure it to change current laws which allow for anonymous bank accounts. The EU claims that the law violates the EU directive on money laundering. Viktor Klima, the finance minister, said Austria was prepared to defend its case at the European Court. Austria is the only country in the EU that allows for anonymous accounts. There are an estimated 26 million accounts. (*Financial Times*, April 10, 1996).

Canada

Ontario Health Minister Jim Wilson announced on Feb. 12 the creation of a combined health card, driver's licence, senior's card and welfare identification card. The new card may use a thumb print electronically scanned into the system. It is expected to be used by all ministries and will cost an estimated $1 billion. (*The Ottawa Citizen*, February 13, 1996).

European Union

American and European direct marketers are lobbying the EU to drop its plans to enact a directive on the privacy of personal information on telecommunications networks. The marketers are urging that the EU allow them to police themselves. (Direct Marketing News Online, May 6, 1996).

Finland

Finnish bank Merita and online merchants have launched a digital cash service using an anonymous digital cash system designed by Amsterdam-based Digicash Inc. Merchants include Internet provider EUnet, the Finnish Securities and Derivatives Exchange and several newspapers, television companies, and online shopping companies. (*Reuters*, March 12, 1996).

France

The National Commission for the Control of Security Interceptions said in its annual report on March 28 that an estimated 100,000 illegal wiretaps were conducted every year in France, mainly by government agencies. It also reported that 15,000 taps are legally authorized each year. (*Reuters*, March 28, 1996).

The Council of Europe ordered France to pay

three French citizens 99,500 francs for illegal wiretaps conducted during the 1980s. (*Reuters*, March 29, 1996).

The French government proposed sweeping changes in the health care system in April 1996. The changes include the requirement that all patients use health care identity cards that would contain their records. Advocates questioned the adequacy of the security of the electronic records. (*New York Times,* April 25, 1996).

Japan

The Home Affairs Ministry announced that it was introducing a 10 digit number which would be issued to all citizens for identification, services, and licensing purposes. Private entities would be prohibited from using the number for other purposes. The numbering will begin in Spring 1999. (*Knight-Ridder*, April 10, 1996).

Lithuania

The Lithuanian Parliament on April 4 voted to allow information about the private lives of politicians to be made public, *BNS* reported. Article 8 was changed to read that such information can be published if it has a bearing on public life. The vote took place during debates on the media bill that started two months ago. Deputies had initially attempted to prevent the publication of details about their, and other officials', private lives. Journalists criticized this stand, accusing them of trying to limit freedom of expression for the sake of protecting their own reputation. The amended article won support from all parties in the parliament. (Dan Ionescu, OMRI Inc., April 5, 1996).

Mexico

The Senate approved a bill on April 1, 1996 that allows the use of wiretaps in criminal cases with the approval of a court, and criminalizes illegal interception of all communications. The bill modifies five provisions of the national constitution. (*Associated Press*, April 2, 1996).

Romania

Nicolae Ulieru, spokesman for the Romanian Intelligence Service (SRI), admitted on May 14 that SRI recorded the private telephone conversations that were played at a conference of the Greater Romania Party one day earlier but said the surveillance had been legal. Ulieru added that Constantin Bucur, the SRI captain who divulged the tape, will be prosecuted for revealing SRI secrets. Also on May 14, the Chamber of Deputies approved a new law on communication, which had been debated in the house for some time before the scandal produced by Bucur's disclosures broke out. The legislation allows eavesdropping on telephone calls under warrant from the Prosecutor-General's Office. (Michael Shafir, OMRI Inc., May 15, 1996).

Spain

The Spanish government has awarded a contract to Motorolla to provide 7 million smartcards for social security. The cards will hold identity and social security information and will require the use of fingerprints to access. By 1999, over 40 million cards will be issued at an estimated cost of $400 million. (*Businesswire*, Feb. 13, 1996).

Uzbekistan

Human Rights Watch/Helsinki issued a report on Uzbekistan in which stated that while "well- publicized arrests, detentions, and beatings of political dissidents" have "decreased markedly," basic civil liberties "remain suspended," *Reuters* reported on May 13. Surveillance of individuals and media censorship are still commonplace. In particular, the organization expressed its concern over measures taken against members of the country's Islamic community. The report comes at a time when foreign governments, including the U.S., have noted an improvement in Uzbekistan's human rights record. (Roger Kangas, OMRI Inc., May 13, 1996).

ADVANCED SURVEILLANCE TECHNOLOGIES CONFERENCE II

Sponsored by

Privacy International
Electronic Privacy Information Center

September 16, 1996

Citadel Ottawa Hotel and Convention Centre
Ottawa, Canada

The rapid evolution of technology is leading to the creation of a seamless web of surveillance across much of the world. Powerful technologies originally developed for the military are being adopted by law enforcement and civilian agencies, and private companies to monitor entire populations. This has been further fueled by the end of the Cold War and increasing demands for greater bureaucratic efficiency. Existing laws and regulations have failed to keep up with these developments.

This one day conference will examine a range of advanced surveillance technologies and their impact on privacy and other civil liberties. It will explore the process of planning and implementation of the technologies, their operating conditions, and the people and organizations responsible for them. The conference will also examine possible technical, regulatory, and legal responses.

The conference will also address in detail the findings of Privacy International's "Big Brother Incorporated" report which examined the international trade in surveillance technology and the involvement of the arms industry.

LIST OF SPEAKERS AND TOPICS

An Introduction to New Surveillance Technologies
- Dave Banisar, Electronic Privacy Information Center & editor, *International Privacy Bulletin*

Tracking the Surveillance Trade
- Simon Davies, London School of Economics & Director, Privacy International

Surveillance Technologies of the Intelligence Agencies
- Mike Frost, former intelligence officer, Canadian Communications Security Establishment & author, *Spyworld*

SIGINT Online: Signals Intelligence on the Net
- Wayne Madsen, author, *Handbook of Personal Data Protection*

Datamining the Net: Cookies, Crawlers and Trackers
- Simson L. Garfinkel, author, *Practical Unix and Internet Security*

Intelligent Vehicles and Tracking
- Phil Agre, University of California, San Diego

Its all in the Genes: The Human Genome Project and Privacy
- Pierrot Peladeau, Progesta Inc. & editor *Privacy Files*

A Privacy Commissioner Case Study: Introduction of a DNA Profile Databank to New Zealand
- Bruce Slane. New Zealand Privacy Commissioner

The Role of Law in Protecting Privacy: A Comparative Overview
- Colin Bennett, University of Victoria

COSTS

US$175 for Commerical Organizations/Government Agencies
US$75 for Individuals/Non-profit Organizations

More information on the conference is available at the PI Home Page at http://www.privacy.org/pi/conference/ottawa/or contact pi@privacy.org. A mailing list for future information is available at pi-news@privacy.org (subject: subscribe).

About Privacy International

Privacy International is a human rights organization concerned with privacy, surveillance and data protection issues worldwide. It has members in over forty countries and is based in London, England with offices in Washington, D.C. and Sydney, Australia. PI has engaged in numerous campaigns on privacy issues, publishes the International Privacy Bulletin, and sponsors yearly conferences. It also conducts studies and releases reports.

PI was formed in 1990 when, in response to a growing number of privacy threats, more than a hundred leading privacy experts and human rights organizations linked arms to form a world organization for the protection of privacy. Members of the new body, including computer professionals, academics, lawyers, journalists, jurists and human rights activists, had a common interest in promoting an international understanding of the importance of privacy and data protection. Meetings of the group were held throughout that year in North America, Europe, Asia and the South Pacific, and members agreed to work toward the establishment of effective privacy protection throughout the world. Since then, PI has held meetings in Sydney, Washington, Manchester, Chicago, San Francisco, The Hague and Copenhagen. In 1992, PI began publishing the International Privacy Bulletin, a quarterly journal of scholarship and updates on privacy issues worldwide.

PRIVACY INTERNATIONAL/INTERNATIONAL PRIVACY BULLETIN

MEMBERSHIP/SUBSCRIPTION FORM

Name/Contact.....

Organization.....

Address.....

.....

Telephone.....Fax.....

Electronic mail address.....

Special interests.

- ○ $US 75 - Personal membership/subscription
- ○ $US 125 - Library/government agency subscription
- ○ $US 200 - Commerical organization subscription

Please make checks payable in $US and send to:

Privacy International c/o EPIC
666 Pennsylvania Avenue, Suite 301
Washington, D.C. 20003 U.S.A.

All information will be held in strict confidence and will not be disclosed without your prior permission.