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

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

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

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

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,

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

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

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

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,

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).

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).

OMRI material was reprinted with permission of the Open Media Research Institute, a nonprofit organization with research offices in Prague, Czech Republic. For more information on OMRI publications, please write to: info@omri.cz.

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.