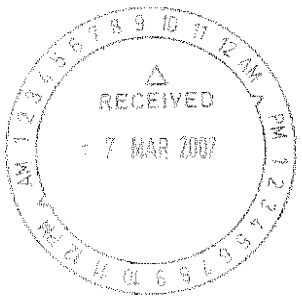
6 March 2007



Mr Alistair Sands
Secretary
Standing Committee on Finance and
Public Administration
Parliament House
CANBERRA ACT 2600

Dear Mr Sands

There are several key issues that need to be addressed in relation to the proposed Access Card to make it acceptable to the Australian community. Unfortunately, the Access Card initiative has been rushed through and many of the community's concerns have been left unaddressed.

In reality, only a fraction of population at large is aware of the proposal, with few realizing exactly what the proposal entails and, as the initiative is discussed throughout the community, further concerns are forthcoming.

Some of these concerns include:

- The Government has no mandate for this proposal
- The Access Card will inevitably become an ID card
- The functionality of the card will increase
- Costs will blow out, and the anticipated benefits may not materialise; and as a consequence the initiative will not yield the benefits the government expects
- There will be breaches of privacy
- Australians should be given a genuine "opt out" capability

1 No mandate for the proposal

The Access Card initiative was proposed after the last election, and was not foreshadowed in the Government's policy announcements in the lead-up to the 2004 election. As such the Government has no mandate for this initiative.

Worse still, many in the community believed that the Government's position in 1988, when the Coalition opposed a similar initiative, remained current.
Given the significance of this initiative and the concerns from many in the community, the initiative should be deferred at least until after the next election when a mandate can be secured. Such a deferral would also give the community time to discuss and analyse in detail what is involved in the proposal.

Recommendation

- **That further work on the Access card be deferred until after the next election when the Government has a mandate for the programme and greater community consultation has occurred.**

2 The access card will inevitably become an ID card

The Government constantly claims that the access card is not to be used as in ID card. If that is the case, why there is a need for a photograph on the card?

If the card is simply to be used for accessing government benefits, a digitised photograph, which is embedded in the chip, would be sufficient for identification purposes when the card is presented to appropriate authorities, eg Centrelink, at a doctor's surgery, or at a pharmacy, as each would have a scanner. Removal of the photograph from the surface of the card would have no impact on the declared functionality of the card, but would ensure that the card could not morph into an identity card.

The problem with the Access Card in its current form is that, once implemented, the infrastructure is in place for the card to become an ID card. All that would be required is a small change to legislation, which, no doubt will be introduced by a future Government.

Finally, the reassurances often cited that legislation would make it illegal for a third party to ask to see the Access Card sound hollow. Currently, it is illegal in several States for third parties to ask to see a driver's licence, yet post offices, clubs and airlines all demand to view drivers' licences on a regular basis.

The only way to stop an Access Card being used in a similar way is to remove the photograph from the face of the card.

Recommendation

- **It is recommended that the photograph be removed from the surface of the card to ensure the Access Card cannot morph in to an identity card.**

3 *The functionality of the card will increase*

Experience shows that linking of databases increases over time – it does not decrease.

One of the major concerns is that the functionality of this card will increase over time. In these circumstances, the card ceases to be optional – it will be mandatory. Worryingly, the Office of the Access Card has indicated that there will be no increase in functionality "at this point in time". Translated this means that the Office of the Access Card does have plans for a future increment in the card's functionality.

There is a huge number of Government programmes that could be incorporated into the Access Card including:

- First home owners' scheme
- Receipt of government grants – eg payments under the Water plan to farmers; Export Market Development Grants;
- Drought assistance payments
- Bushfire relief payments
- Isolated Children's Allowance payments
- Taxation information.

Many of these programmes particularly impact on the farming community and on our regional areas.

The bottom line is simply that once the infrastructure is in place, Governments will be sorely tempted to increase functionality, bringing together all aspects of an individual's life under one identity number. It will be practically impossible to live in Australia without a card.

4 *Costs will blow out*

The proposed Access Card has been justified primarily on the grounds that the reduced levels of fraud justify the costs associated with its introduction. A full cost-benefit analysis has not been released by the Government (including sensitivity testing), yet it is clear that a relatively small increase in the costs or a reduction in anticipated benefits, will result in the project ceasing to be cost effective. Indeed the Government has refused to release the PriceWaterhouseCoopers report on the Access Card, which covers some of these issues, despite FOI requests.

History has shown that large-scale government information technology purchases always:

- cost much more than originally promised;
- invariably run years late;
- have large scale transitional implementation problems; and ultimately

- cause political difficulties at least at the time of introduction.

The current Government experienced exactly these problems with the contracting out of Commonwealth Government IT services from 1996 – eventually culminating in the Humphries Review.

The Customs IT system is another example of a ten-fold blowout in costs. When the system was finally introduced it caused a crisis on the docks, a serious disruption to trade, large compensation costs against the Commonwealth and some border security lapses.

The State Governments also have a string of such failures. One contemporary one is the proposed public transport smartcard in NSW. This has been delayed again recently by the Premier. Many other States have experienced the same problems.

In addition, the claimed savings from reducing welfare fraud are not considered to be robust. There are already significant anti-fraud systems in place in the Commonwealth welfare system. For example, few people object to data matching between the Tax Office and Centrelink concerning welfare fraud. Accordingly, this practice has massively expanded over the past 20 years as computer systems have become more sophisticated. This practice has already cut down on a lot of welfare and taxation fraud. It is a cliché, but nonetheless true that you cannot make the same saving twice.

The concern is that once the process is commenced, the sunk costs of the Government become so high that it cannot afford to pull out, lest a scandal develops in relation to the waste of resources.

Recommendation

- **Further substantive work on the Access Card be deferred until the government can be assured costs will not blow out and the initiative will be cost-effective.**

5 *Breaches of privacy*

Even if all of the other problems did not exist (and they are very real), in the end privacy and protection of the public interest always rely on the Government employees doing the right thing.

Whilst the overwhelming majority of public servants are highly ethical, hard working, law abiding people – there are always going to be people who do the wrong thing.

And there are countless examples of where this has happened (see Attachments 1 & 2)

Just recently, several public servants at Centrelink were caught misusing confidential personal information. Some 585 staff were sanctioned for privacy violations, 19 staff were dismissed and 92 had resigned (see attached media report about one such incident).

But the problems are much deeper than this. In the Child Support Agency some 405 breaches of privacy were discovered, including 69 cases where sensitive information was given to former spouses.

In Medicare Australia, there have been 21 cases of privacy breaches in recent times. Five staff were counselled, two demoted, eight have resigned and six were terminated.

There are probably countless other privacy breaches which have not found their way to the public domain. Storing a huge amount of data about a person will also increase the risk of identity theft – either through the card being stolen and the data being accessed or through hacking of the central databases which store all of the backup information.

What needs to be recognised here is that creating more databases with more information and greater centralisation will inevitably increase the risk of misuse of the data. And it will happen.

There are two issues here. First, what compensation does the Government propose should be paid to those people who have been forced to provide information to Government as part of the Access Card program, and having done so in good faith find that their personal information has been compromised? If there is a policy of no compensation, that matter should be expressed admitted by the Government and be allowed to be publicly debated. What about the situation where someone comes to physical or other harm due to the disclosure of private information, including an address, where someone is trying to avoid detection by a third party, eg an estranged spouse?

And secondly, does the Government intend to notify individuals when there has been a breach and their personal information disclosed? If so, what details will be made available, will the relevant officer who committed the breach be accountable to the citizen etc?

6 Opting out

There are many in the community who are genuinely concerned about the Access Card and many of these would be traditional Coalition voters who supported the Coalition's position in 1988. They are worried about some or all of the above factors including that the Access Card will become an ID card, the demonstrable lack of privacy in government databases, and general potential misuse of the database by government agencies and the facilitation of big government through the use of the Access Card. They are concerned that the use of the Card could extend over time to state and local services eg, public transport passes, public dental services, community childcare services and library services.

Many Australian simply want to be able to opt out of this identification system, and that as detailed knowledge of the Access Card proposal progressively grows it is likely that many more will want an opt-out option.

The philosophy behind the opt-out option is straightforward.

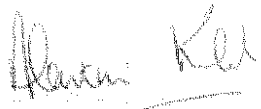
Those Australian tax payers who pay the Medicare levy (which is a national health insurance system), and who do not wish to draw welfare benefits or be involved in the huge inter-linked data system should be able to opt out. As such these Australians would not be able to claim the Medicare rebate or other rebates through the Access Card system. In return these Australian citizens should be entitled to income tax deductibility on the additional personal medical expenses that they incur. Under this approach the Government would still be financially better off than providing the direct benefit but those opting out of the National Identification System, would be entitled to some taxation benefits and would not be expected to fully fund all the costs of their medical care.

Recommendation

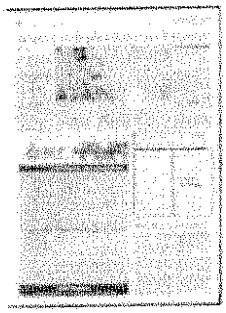
- **Citizens to be entitled to "opt-out" of the Access Card system and be entitled to income tax deductibility for all Government services subsidies that they consequently forfeit.**

I would be pleased to further elaborate on the above submission, should you wish.

Yours sincerely



(Alastair Kinloch)



Australian Financial Review
Friday 25/8/2006
Page: 32
Section: General News
Region: National Circulation: 85,843
Type: National
Size: 105.04 sq.cms.
Published: MTWTFS

Brie

Prying staff cast doubt on smartcard security

Privacy advocates have serious concerns about the federal government's proposed smartcard after Centrelink staff were caught inappropriately accessing client records.

Using sophisticated spyware programs, 600 Centrelink staff were caught browsing the welfare records of friends, family, neighbours and ex-lovers without authorisation.

Nineteen Centrelink staff were sacked and 92 resigned after 790 cases of inappropriate access were uncovered.

The head of a privacy taskforce looking into the government's proposed health and welfare smartcard, Allan Fels, said he was deeply concerned about the implications for Australians.

The smartcard will link medical, tax, welfare and other personal details on at least 17 million Australians.

"The Centrelink revelations are deeply disturbing," Professor Fels told ABC radio yesterday.

"I take some comfort from the fact that the government has caught them and punished them, but there is still a huge weight now on the government to provide full, proper legal and technical protection of privacy with the access card."

Centrelink said five cases had been referred to the Australian Federal Police and more than 300

"The Centrelink revelations are deeply disturbing."

staff faced salary deductions or fines. Another 46 were reprimanded, and the remainder demoted or warned.

The Labor Party said the breaches demonstrated the government's administrative incompetence and that the privacy commissioner should investigate.

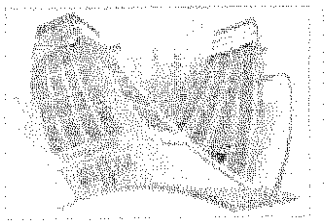
AAP

Print | Close

Saturday, 26 August 2006

Eyeing Big Brother

Paul Malone



The latest privacy breaches of government records raise new questions about plans for a national smart card for 2008. PAUL MALONE reports

LIKE THE universe, the government's share of our information is exploding: birth dates, income and tax records, health information, the census, criminal records, marriage and family details, unemployment benefits, traffic infringements, disabilities, death records. The list of some of our most intimate data gathering on official files gets bigger by the day.

Public servants, bound by codes of conduct and threatened with the Crimes Act and secrecy provisions, are the keepers of the files. Tens of thousands of public servants have access to databases with information about you and me. In the Defence Department alone there more than 10,000 staff who are certified users of the personnel-management system that held the records of all Defence staff.

But it is in agencies such as Centrelink, the Australian Taxation Office and Medicare Australia - where records on the vast majority of Australians are held - that there is the potential for abuse that could affect any one of us.

The revelation this week that 585 Centrelink staff had been sanctioned for privacy violations, that 19 had been dismissed and 92 had resigned as a result brought the issue to the public's attention.

But the Centrelink cases are not unique. Earlier this year it was revealed that the Child Support Agency had discovered 405 breaches of privacy, including 69 cases where sensitive information was given to former spouses.

In Medicare Australia, where 5400 staff are employed, over the past three years a total of 21 cases of privacy breaches, unauthorised access or fraud have been identified. Five staff were formally counselled, two demoted, eight resigned and six were terminated.

A further 13 cases are under investigation.

And in November last year an Immigration Department employee was convicted in the ACT Magistrates Court on 16 charges of unauthorised access to client records.

The agencies with the biggest potential for invasion of privacy are the tax office and the big two in the Human Services portfolio, Centrelink and Medicare.

In confirming the breaches of privacy at Centrelink, the chief executive, Jeff Whalan, presented the best possible spin, saying his organisation had boosted privacy protection. The general manager of Centrelink, Hank Jorgen, was keen to emphasise that Centrelink had initiated the investigation.

But the chief executive of Civil Liberties Australia, Bill Rowlings, observed that if they had caught one or two people you would say, "OK, somebody's done the wrong thing."

But close to 600 was another matter altogether.

Whalan made the point that Centrelink has 25,000 staff and the overwhelming majority performed their duties in a highly ethical and responsible manner. But he could hardly be proud of the fact that one in 50 broke the rules.

One of explanations for the relatively high incidence of breaches in Centrelink is that it is only in the past two years that the agency has employed spyware technology to track staff transactions and browsing. Medicare is understood to have had such systems in place for years.

The Child Support Agency breaches - relatively as high as Centrelink's - are even more disturbing, with the possibility that a leak could enable a former spouse to physically harm a former partner.

Privacy Commissioner Karen Curtis says it is unacceptable to have any breach. But it is good news that Centrelink has caught the violators.

"It is good that they've found these and they've done serious things like [having staff] demoted and

dismissed," she says.

"It's really hard. You're always going to find there are some bad eggs and you have to put in place processes to stop those bad eggs."

Since taking the job as Privacy Commissioner she has been impressed with the amount of resources Centrelink has directed towards privacy. Centrelink had been monitoring operations for over a year and had warned staff that it was doing the audit. Interest in the Commonwealth Government's protection of people's records is at a peak at present because of the proposed introduction of the smart card, or access card. Potentially the card could be issued to 17million Australians. Some see it as an identity card, or the revival of the aborted Australia Card.

It is proposed that the card - to be introduced in phases from 2008 - will replace 17 health and social-service cards, including the Medicare card and the veterans' card.

The Government believes it will improve delivery of services to many Australians. Carriage for the card rests with the Department of Human Services, which also has responsibility for Centrelink, the Child Support Agency and Medicare.

What is not widely understood about the card is that its introduction will not mean the consolidation of the databases of the various agencies. Nor will it mean that an officer working with the unemployed in Centrelink will be able to trawl the Medicare data.

In this public-service area, everyone, it seems, is proud to proclaim that "data silos" will be maintained. (Even under present arrangements agency silos are not totally sealed. Under the strictest controls and with legislative approval, Centrelink officers can and do check information on income and tax with the tax office.)

The card will in effect provide users with a key to get into each and every agency. Rather than have a number of cards - Medicare and veterans, for example - the staff at Medicare, or at the Department of Veterans' Affairs, will recognise the access card.

The card will have standard information - the user's name, photograph, digital signature, address, and the access to benefits. To allay fears about privacy, the Government has established the Access Card Consumer and Privacy Task Force, chaired by former Australian Consumer and Competition Commission head Professor Allan Fels.

This week Fels said the Centrelink scandal highlighted why data on the card should be kept to a minimum.

He said the Centrelink revelations were disturbing but he took some comfort from the fact that the Government had caught the breaches.

An expert in the field, the former head of the access-card taskforce, James Kelaher, agrees with Fels that the minimum amount of information should be on the card. But he notes that there are some large groups, seniors, for example, who need, or may want, more information on their card. There was a trade-off. "No information detracts from the card use," he says. "Too much information creates too many problems. There's a spectrum and you've got to be down the end of the spectrum which is not very much on the card."

In her submission to the taskforce, Curtis questions whether the card has to have a photograph. She says a photograph should be printed on the card only if the individual wants it.

"A card with near-universal adult population coverage and having a printed photograph on its face would be close in appearance to a national identity card," she says.

A photograph of the face is not necessary for the card to interact with an electronic reader and for the person's identity to be established when he or she visits a government agency. Curtis wants legislation to limit the use of the card, to prevent unauthorised access or disclosure and prevent routine data matching.

Kelaher says the card is part of a whole new system.

It will replace an antiquated paper-based system with something that will be easier for people to use and easier for people to keep their own information up to date. When it was in place the system would be more secure than that used by the banks for internet banking.

Curtis distinguishes between different levels of improper activity. At the lowest level there is browsing - unacceptable but without the impact on the individual that other actions might have. Then there is getting information to use for non-sanctioned purposes.

At the highest end there are criminal acts such as altering records and fraudulent activities punishable by dismissal and charges.

Curtis notes that the culture in an organisation is an important factor in discouraging breaches of privacy. Staff had to be educated and made aware of their obligations and the limitations on their authority.

If the complaints to the Privacy Commission are a measure, Commonwealth Government activities are not a major privacy area of concern. Curtis says she receives between 1200 and 1300 complaints a year and only 10 to 13 per cent of them relate to the way Commonwealth departments and agencies operate. But complaints go to the commission only if they are not resolved internally. The relatively low number of complaints about government activity might therefore indicate that agencies are better at resolving complaints themselves.

While having staff who do the right thing is the best security, building the technology properly and putting in place systems that can track and monitor transactions increases the chances that staff will do the right thing. A year ago the audit office reported that the Defence personnel-management system, which holds the records of 100,000 people, could be accessed by 10,000 staff. Yesterday the department told The Canberra Times it was 12,000 - but insisted multiple layers of security existed to prevent open access.

At that time the system, known as PMKeyS, did not automatically log a record of those who viewed staff details. The free access could enable identity theft. This week a Defence spokesman said all PMKeyS operators were warned every time they accessed the system that they were subject to the provisions of the Privacy Act and Defence Security Protocols.

Access to personal information was controlled by profiles such as "supervisor" or "personnel officer". These profiles provided the restrictions on transaction and access. The system created audit records for transactions where data was created or changed, including identifying who did the change, the date and what was changed.

The system was independently audited in 2006 and the auditors had stated that the PMKeyS access-management system gave appropriate protection to data.

Curtis said she understood that since last year Defence had introduced better procedures to audit and monitor conduct. But to get a browsing audit trail would require a rebuild of the system. She understood Defence had undertaken to do that.

The card system has yet to be built. Keeping data in silos, giving users tight profiles and having a high-tech monitoring system will provide the basic security. But any system that can be built can be cracked. In the end, an honest staff committed to privacy is the only guarantee of security.

The Canberra Times

Friday, 25 August 2006

Scandal highlights privacy shortfalls

THE REVELATION this week that hundreds of Centrelink staff have been caught inappropriately accessing client records is another worrying reminder that government departments are falling well short of adequate standards of administration and privacy protection.

The breaches of Centrelink's computer database, which contains the records of all welfare recipients in Australia as well as people's work and living arrangements, were widespread and alarming. A two-year internal audit using spyware computer technology showed that staff had accessed customer records on hundreds of occasions - with many browsing the files of neighbours, friends, family and ex-spouses. Of those who were caught, more than 300 were fined or had their salary reduced, 19 were dismissed, and 92 resigned when challenged about the breaches. Five cases have been referred to the Australian Federal Police.

Centrelink claims that the numbers of those caught in the sweep comprise only 2 per cent of the department's workforce and that no information found its way into the public domain. Centrelink's manager, Hank Jongan, insists that his agency has a policy of zero tolerance when it comes to breaches of privacy, but can the public accept this assurance that sensitive information cannot fall into the wrong hands?

It was only in June that an internal audit commissioned by the Child Support Agency found 405 instances of privacy breaches, all within a nine-month period. Some 69 of those cases involved information being given to ex-spouses. That such security lapses have been revealed in an agency dealing with highly sensitive issues is worrying, as is the comment of the auditors that such breaches many indicate others "not yet brought to light".

The minister in charge of both agencies, Joe Hockey, has said he's satisfied with the action being taken by Centrelink and the CSA to ensure such lapses do not occur again, but nonetheless, the public has grounds for believing that perhaps government is not doing enough to ensure that the Public Service upholds the highest privacy standards.

This newspaper reported yesterday that Medicare Australia plans to investigate and strengthen its privacy protection arrangements, and while there is no suggestion it has experienced the kinds of problems unearthed at Centrelink, few other agencies and departments bother to promote their efforts or reassure the public that they have the capacity to prevent sensitive information being accessed by unauthorised personnel.

If the bungling at Centrelink and the CSA raises questions about the general integrity of the Public Service, its also raises doubts about the Government's ability to deliver on its promise of a safe and secure access card for health and welfare recipients. Implementation of the card, scheduled for 2008, is another of Hockey's responsibilities.

In the wake of the Centrelink revelations, the chairman of the Government's task force on the smart card, Professor Allan Fels, said the Government had to refocus its efforts to ensure the card contained all the measures necessary to protect people's privacy.

His doubts echo those of the previous chairman of the task force, James Kelaher, who resigned in May after Hockey rejected his concerns about privacy and the way the card was being implemented. Kelaher felt that the project, and the administration of the card, should be independent of the Department of Human Services or at least outside the purview of Centrelink and Medicare - the two agencies that deliver the bulk of welfare and health benefits. He also wanted a panel of external experts to advise the Government on privacy protection. But Hockey ruled out any new approach, saying the Government could satisfy people's privacy concerns without external advice.

Hockey and the Government appear confident that emerging technology will deliver a card that will not only carry extremely sensitive biometric data, a digitised photograph and a chip with an encrypted identification number, but will enable access to all data stores now held separately by government departments - all this without the risk that any unauthorised third parties could fraudulently gain access to that information through identity theft or computer phishing. But no matter how technologically sophisticated a card might be, there are sound, historical reason for believing that criminal or rogue elements will quickly bridge that gap.

Most people would accept that a tamper-proof access card is a practical impossibility, just as they know there will always be one or two public servant tempted to fraudulently obtain information for profit or curiosity. But if the public loses confidence in the ability of government to do all it can to protect people's privacy, they will be reluctant buyers of any access card.

The Centrelink scandal suggests that Hockey has more work to do to convince people that government can indeed be trusted to plug the privacy gaps.

The Canberra Times

Print | Close

Thursday, 24 August 2006

PS acts to track privacy snoops

Paul Malone

Medicare Australia will be investigated for privacy breaches after hundreds of Centrelink staff were found to have been illegally spying on the records of welfare recipients.

The Child Support Agency - which holds the highly sensitive records of divorced couples - will also come under renewed examination. And the departments of Defence and Immigration are overhauling their computer systems to track data snoops.

The wholesale breaches have also called into question the security of the proposed health and social-services access card, which would replace 17 health and social-services cards, including the Medicare card, health-care cards and veteran cards.

The Centrelink dragnet resulted in 585 staff being sanctioned for code-of-conduct violations. Department head Jeff Whalan said yesterday that 19 staff had been dismissed and another 92 had resigned when challenged about breaches of privacy.

More than 300 had been fined or had their salary reduced with the bulk of the rest receiving demotions, reprimands or warnings.

The Centrelink incidents follow similar instances at the Child Support Agency where earlier this year 405 breaches were uncovered. Of these, 69 involved sensitive information being given to ex-spouses.

Centrelink, the Child Support Agency and Medicare all fall under the control of the Minister for Human Services, Joe Hockey. Mr Hockey was visiting indigenous people in remote regions yesterday and was not available for comment.

A spokeswoman for Mr Hockey said Medicare Australia was looking at what Centrelink had done in monitoring its staff to identify breaches. She said it was her understanding that the sort of issues that came up in Centrelink did not seem to exist in Medicare.

However, because of the strong stand Mr Hockey had taken on privacy, Medicare was working with consultants to look at how it could strengthen privacy protection.

Earlier this year CSA undertook an independent review of its operations. The review found the potential for identity theft, people gaining contact details which might enable them to find and harm former partners and inappropriate access to prominent identities.

The minister's spokeswoman said 95 per cent of the review's recommendations had been adopted and were being implemented. Mr Hockey had supported his agencies in taking strong action in addressing the privacy problem and this was now bearing fruit.

He had zero tolerance when it came to staff inappropriately accessing customer information and supported a tough line against people doing the wrong thing.

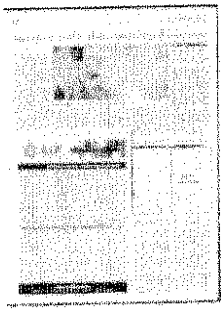
Privacy is a major issue in Mr Hockey's portfolio as he is responsible for the introduction of the health and social-services access card.

The shadow minister for public accountability, Kelvin Thompson, said the Centrelink and CSA breaches were clear evidence that Mr Hockey was neglecting his department and Australians were paying with their privacy.

"It is time the Privacy Commission stepped in to sort out Hockey's mess," he said.

The news also raised privacy concerns about the smartcard project that would affect the privacy of 17 million Australians. The smart-card would hold extremely sensitive data such as biometric photographs and signatures.

The Canberra Times



Australian Financial Review
Friday 25/8/2006
Page: 32
Section: General News
Region: National Circulation: 85,843
Type: National
Size: 105.04 sq.cms.
Published: MTWTFS

Brie

Prying staff cast doubt on smartcard security

Privacy advocates have serious concerns about the federal government's proposed smartcard after Centrelink staff were caught inappropriately accessing client records.

Using sophisticated spyware programs, 600 Centrelink staff were caught browsing the welfare records of friends, family, neighbours and ex-lovers without authorisation.

Nineteen Centrelink staff were sacked and 92 resigned after 790 cases of inappropriate access were uncovered.

The head of a privacy taskforce looking into the government's proposed health and welfare smartcard, Allan Fels, said he was deeply concerned about the implications for Australians.

The smartcard will link medical, tax, welfare and other personal details on at least 17 million Australians.

"The Centrelink revelations are deeply disturbing," Professor Fels told ABC radio yesterday.

"I take some comfort from the fact that the government has caught them and punished them, but there is still a huge weight now on the government to provide full, proper legal and technical protection of privacy with the access card."

Centrelink said five cases had been referred to the Australian Federal Police and more than 300

"The Centrelink revelations are deeply disturbing."

staff faced salary deductions or fines. Another 46 were reprimanded, and the remainder demoted or warned.

The Labor Party said the breaches demonstrated the government's administrative incompetence and that the privacy commissioner should investigate.

AAP