Will this Election be an Honest Election?

Dr Amy McGrath, 12 September 2004

Whether this election can be honest is now the second hottest topic with callers on talk-back radio according to media monitor, *Rehame* out of their top ten, according to a news item in the *Courier Mail* of Friday, September 10 hot topics. It comes second only to the topic of the federal election in general.

This will no doubt astonish all our pollsters, as it had never rated a mention until now; as will the fact that nationally it displaces in order interest rates, Mark Latham, the Wentworth preselection, political advertising, children overboard, tax policies and media bias.

Therefore this coming election of 9 October 2004 is not solely about 'Honest John'. It is also about whether it will be an honest election, as it will be a 'crisis' election - one that is measuring up as a 'do-or-die' election.

Each time there has been a 'crisis' election, as in 1987 and 1993, grave misgivings and doubts about the election results have arisen. This 2004 election promises to be similar. It has the same feature - a gateway has been created allowing theft of votes and results in selected electorates and hence even the election itself.

In 1987 it was a total new system of running the election and vote count which caused chaos and confusion. In 1993 it was the launch of the Australian Electoral Commission's ELMS system for management systems just before the election, followed by severe disruption of the entire system for weeks before and after the election.

In 2004, a new gateway has been created by outsourcing the management of the AEC's information centre to Call Centres of Centrelink in all States which will operate from issues of the writs to two weeks after polling day. In 2007, the AEC will have only one Call Centre for all Australia.

Scarcely anyone would give a second's thought to that arrangement. Helping people to know about their enrolments, and how and where to enrol and vote, what's wrong with that? Everything. The Call Centres, already under fire for inefficiency, are not on AEC territory, but in separate buildings. They are manned by casuals. Hundreds of them? In different languages? Only one question asked - 'have you engaged in political activity?

Currently Divisional Returning Officers are troubled that these casuals will be linked by terminals to the mainframe data base of the AEC already outsourced to Computer Services Company, presumably to check enrolments. The legality of this is arguably questionable in terms of the Commonwealth Electoral Act.

Divisional Returning Officers and AEC Head Office staff in various states would prefer to have such casuals, often locals recruited through successive elections, working with them as has always been the case. Then they can keep an eye on trends and problems of irregularities or fraud only obvious to anyone familiar with the electors in their neighbourhood.

I was further troubled about these new Call Centres when I happened to read a short paragraph buried in a routine article by the Chief Political Correspondent of the *Sydney Morning Herald*, Louise Dodson. This stated that the AEC were hiring casuals "to oversee the electoral roll and vote count."

Now that oversight is the statutory role of experienced Divisional Returning Officers in each electorate. My first reaction was that the AEC could surely not have made such an elementary mistake as to announce that their roles would be delegated to others in any way. I rang Louise Dodson. She assured me that is exactly what their spokesman had told her.

I rang Mr Dyak, overseeing those casuals, who denied the AEC had said that. The casuals would only be answering enquiries. For this they would need access to the electoral roll. As Louise Dodson is a seasoned reporter of high repute, I was left to speculate if the AEC spokesman had let slip some aspect of the change to a Call Centre the AEC had preferred unknown.

Mr Dyak sought to set my concerns at rest by saying the casuals would have a Reader Only Access Bar on their computer link to the database. The implication of this is that no one could fraudulently stack that roll. He did not deny that they would be linked to the database.

Now a Reader Only Access Bar is a very flimsy barrier as any computer expert will tell you, aware that such very high security systems, as the Pentagon, the British Communications Satellite and even Microsoft itself, have been breached. Reliance on the Bar to prevent fraud is very dangerous. It could be bypassed by any technician called in to 'fix' a machine because he would need passwords to do so. It could also be bypassed by any casuals planted there, armed with the passwords, with evil intent.

What if someone did bypass the terminals in the Call Centres? He or she could perpetrate the most common successful fraud by stacking the electoral roll in marginal seats in bulk with illegal 'ghost' names and addresses, or names moved from safe seats as re-enrolments during the 5 weeks between close of rolls on September 7 and polling day on October 9.

The electoral rolls printed immediately after the close of rolls on September 7 are the tools for marking off voters' names in order to issue them with ballot papers on October 9. A false assumption is often made that these rolls cannot be stacked with illegal names after the close of roll on September 7. That is not true.

If stacked after the close of roll on September 7, such illegal names could be stacked onto the electoral rolls that Divisional Returning Officers call up in their electorate offices to check and mark off the validity of postal and pre-poll votes for they have not been marked off on the rolls used in the polling booths on polling day since 1984.

If you are sceptical that such a scam would succeed, you may not be aware the floods of these 'declaration' votes are enormous, and the public and media pressure great, to deliver results in two weeks of the former four. The result is that Divisional Returning Officers are no longer required to check the validity of all of them. They are only spot-checked. The more there are, the fewer are checked.

Any 'artful dodger' could work that scam to deliver late postal votes in those names to stack a result. All he needs is a stack of those postal vote application forms the major parties so blindly flood on the market, and use his 'ghost' names. Get his postal vote. Witness it, send it in after the four days still allowed - only if the count is tight in the seat he is targeting.

The AEC spokesman told me some casuals in the CentreLink Call Centre will be working for two weeks after polling day. That creates the possibility that anyone, who may have used the Call Centre as a gateway to such fraud, could delete the fraudulent names as simply as they were added.

I remind any doubters that over 100,000 names were removed from the roll immediately after the 1987 election from the 715,000 names enrolled immediately before. After a break in TV transmission in the vote count, a uniform swing in the vote for the ALP occurred in the marginals - compared to a swing against it overall, and of 1% in the two-party preferred count - delivered it government.

Also a computer hacker, Timothy Cooper, hacked into the AEC system just after RMANS was operable which was just before issue of the writs for the March 1993 election. As the prosecutor for the AEC in his trial in the Brisbane District Court on 27 December, 1996 said "he had gained access to the system at the highest level' which would have enabled him to install programs and alter existing programs and data in the system."

He was able to enter the electoral roll and vote count and leave no trace. The disruption throughout the election interfered with the ability of the Divisional Returning Officers to enter enrolments and the Senate count.

We can't know whether results had been swung. In the upshot, the ALP won that election by 1452 votes in 16 electorates.

As Professor Micco, a lecturer in the graduate program for the US Congress on electronic fraud in e-banking and e-commerce of the University of Pennsylvania, said in speaking to the HS Chapman Society "truthfully any system can be hacked. So both insider and outsider hackers are possible, but actually 90% of the computer crime is done by insiders."

Is the AEC being irresponsible in creating such a gateway to fraud as this Centrelink Call Centre? Can the AEC's assurances that its systems are 100% secure from hacking fraud be believed when it will have no supervisors there? I have scrapbooks full of experts in the US and our media constantly saying "No".

Mr Duggie warned in the *New Yorker* on November 7, 1988: 'The practical problem of the computer is its invisibility. Whether or not elections have been stolen by computer before, some citizens and some officials are asking if it could happen in the future. Could people acting for political reasons or personal gain, steal House of Senate seats, or even the White House itself?'

Exactly! The warning is clear. We could have another computer hacker via a Call Centre in 2004?