Submission 084
Date received: 01/03/14

SC

1 March 2014

Please accept this submission to the Inquiry into the 2013 Federal Election.

My concern relates to the applications for postal voting that were distributed by the Labor and Liberal parties prior to the 2013 election. The postal vote applications printed by these parties encouraged the voter to return the application to the party office in the addressed envelopes included with each application. The problem is that the postal vote application requires the applicant to provide a security question and answer that are used by the AEC to verify the postal vote once it is cast. Allowing the postal vote application to be returned to a political party instead of the AEC means that neither the security question nor answer is secure.

Once the postal vote application is opened by Liberal or Labor Party staff, the security question and answer is accessible to them. This means that postal votes as a whole cannot be deemed secure applications returned to party offices were accessed by any number of unknown persons prior to the AEC receiving the application. Postal votes cannot be secure when the security questions and answers could be known or changed by political party staff.

My family received postal vote applications from both the Labor and Liberal Parties prior to the 2013 election. I personally examined these postal vote applications, and it is to them that I refer to in this submission. I am unaware if other political parties engage in this practice.

Although no-one in my family planned to cast a postal vote, when I first saw the postal vote applications, I noticed immediately that the application asked for a security question and answer, yet the application could be returned to either the Labor or Liberal Party office instead of the AEC. The Liberal Party application envelope was addressed to a Liberal Party office called the Postal Vote Centre at a reply paid address in Sydney South, and the Labor Party envelope was addressed to David Bradbury's office in Penrith NSW. I was concerned about the path the postal vote application would take, so I contacted these two offices on the number provided within the application. Staff at each office told me that after the postal vote applications were received by them, the applications were opened and the contact details of the applicant were harvested. Staff saved the contact details from each application for use by the party to send out how to vote cards. The applications were then sent on to the AEC. This was true for both parties.

After hearing this, I looked carefully at each application, looking for any form of consent to application details being harvested by party staff. I was unable to find anywhere on the application where consent was asked for or given regarding any political party harvesting contact details from the application. This seemed unethical at best or illegal at worst.

The far great problem, however, is that since staff at each party office opened the postal vote applications to get the contact details, they also had access to the security question and answer. This security question and answer is used by the AEC to verify the postal vote once it is cast. Since the possibility exists that the various office staff know the security questions and answers of all postal vote applications that pass through their offices, the security questions and answers are no longer secure. There exists the possibility that a postal vote applicant's vote could be either hijacked or discounted if someone either votes in their stead or submits a second ballot using their security answer. There is also the possibility that the security question or answer could be changed by someone unauthorised to do so, preventing postal voters from having their vote count.

We might well say that no-one would ever knowingly change or destroy someone's vote. And I do not mean to imply that any current or former office staff at the two offices I contacted would ever do such a thing. But the vote of an individual counts, and the votes of many individuals can change the future. We must insure that every vote counts and that every vote is secure.

Allowing any organisation other than the impartial AEC to access postal vote application material with sensitive information is a security risk to the electoral system. A simple fix to the problem would be to require that all postal vote applications be returned to the AEC directly instead of to a political party. An even greater fix would be to have electoral material printed, delivered, and received only by the AEC.

Thank you for this opportunity to make a submission.

Submitted by:

Susan Moisiadis