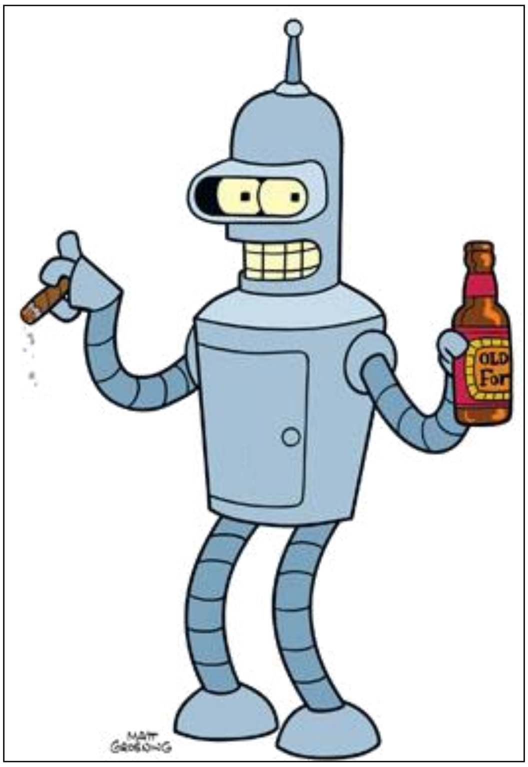
The greatest threat to democracy
By Niraj Lal

April 2013



In 2010, Washington D.C. elected a robot to public office. This robot wasn't a bland product of party politics, nor a computer calculating the greatest good for the greatest number, but Bender Bending Rodriguez - the drunken suicidal robot from *Futurama*, a cartoon series by the creators of *The Simpsons.*

The election was run by the Washington D.C. Board of Elections and Ethics as a trial of the world's most secure and advanced electronic voting system. The trial was held a month before the system would elect, in earnest, officials to the Washington D.C. School Board. The board invited the world to attack the system as a public demonstration of its security.

Within hours of the trial going live, the system was hacked. Every vote was stolen from the real candidates, every candidate was deleted from the register, Bender[1] was installed as the sole voting option and was duly elected unanimously. Not only was the voting system compromised, the hackers were able to identify the names, addresses and votes of every (real) registered voter and change the password to lock out election officials from the system. The breach wasn't noticed until two days into the election trial, and might have gone undetected for longer had the hackers not left a calling card on the thankyou-for-voting page consisting of the word "OWNED" in bold, and a victory song played from the webpage. Once the infiltration was detected, the hackers were able to watch the confusion unfold through the internal camera system of the Office of the Election Board.

The successful hackers weren't a collection of masked individuals from Anonymous, nor scientists from Iran (though both were trying), but a computer security research team from the University of Michigan led by Assistant Professor J Alex Halderman. The research is described in a beautifully written paper[2] in the proceedings of the 16th Conference on Financial Cryptography & Data Security, 2012. The actual hack arose from the accidental use of single quotes (') instead of double quotes (") in the shell script of the server, but the researchers identify that even in the best code "…mistakes like this are all too common. They are also extremely hard to eradicate, not because of their complexity, but because of the multitude of potential places they can exist". They argue that "web application frameworks tend to be *brittle*"[3]. The conclusion: "Securing Internet voting in practice will require significant fundamental advances in computer security, and we urge Internet voting proponents to reconsider deployment until and unless major breakthroughs are achieved."

An earlier study[4] led by Dr David Jefferson from the Lawrence Livermore National Laboratory in the US noted that: "These vulnerabilities are fundamental in the architecture of the Internet and of the PC

[1] Image by Comedy Central, available from wikicommons.

[2] S Wolchok, E Wustrow, D Isabel and J. Halderman, 'Attacking the Washington D.C. internet voting system', In Proc. 16th Conference on Financial Cryptography & Data Security, Feb. 2012,
freely available here: https://jhalderm.com/pub/papers/dcvoting-fc12.pdf

[3] their emphasis.

[4] D Jefferson, A Rubin, B Simons, D Wagner, 'A security analysis of the secure electronic registration and voting experiment', Commisioned by the US Government, Jan 2004.
freely available here: http://servesecurityreport.org/paper.pdf

hardware and software that is ubiquitous today…Such attacks could occur on a large-scale, and could be launched by anyone from a disaffected lone individual to a well-financed enemy agency outside the reach of... law." The study sternly recommended: "Shutting down the development of the US Secure Electronic Registration and Voting Experiment immediately and not attempting anything like it in the future until both the Internet and the world's home computer infrastructure have been fundamentally redesigned, or some other unforeseen security breakthroughs appear.".

There are two main supporting reasons for electronic voting: 1) Quicker counting of ballots and 2) Easier voting for citizens unable to attend a polling station.

Considering first the speed of counting. The 2009 Federal Election took the longest to decide of any Australian Election, with a total of 17 days before a government was formed. This time was due to the counting of postal ballots, recounting of votes in critical electorates, and negotiations between elected members to form government, since no political party had won a clear majority. Looking to similar Westminster systems around the world, this is increasingly likely to happen. During the election period, parliament enters caretaker mode – defined by legislation outlining the roles and responsibilities of government during this period. With electronic voting, this period would be shortened. Electronic voting guarantees near instantaneous counting of results. Polling results would likely be declared soon after voting closes in Western Australia. But the electronic counting of votes comes with its own risks – the most significant of which is the loss of ability of the general public to scrutinise votes and the counting of ballots. With the current paper ballots, any member of the public is able to scrutinise Australian Electoral Commission officials as they count votes in every polling booth in the country. The only intellectual capacity required is that the scrutineer can recognise numbers, read names, and count.

With electronic voting, the verification of counting can only be achieved by computer experts. Even if the source code of the system were 'open source', that is – if the software and algorithms were published for open scrutiny (which they must be – otherwise how could we trust them at all?) – the ability to scrutinise code is limited to a vastly smaller number of people. The scrutineering process will move towards a system based on trust of computer experts and the people that hire them. Australia currently has strict rules regarding the roles and responsibilities of caretaker governments which to date have not been disputed nor have been a cause for concern. The dangerous loss of the ability of the general public to scrutinise votes does not overweigh the speed of counting that electronic voting promises.

Internet voting offers ease of access to voters unable to attend a polling station on election day. This includes military personnel serving overseas, elderly and disabled citizens, Australian citizens abroad and Australians living in remote communities. Making voting easier is especially important in countries without compulsory voting, helping to 'bring out the vote' and increase the number of total votes cast. Voting is compulsory in Australia, and as a result, the Australian Electoral Commission is charged with the responsibility to make voting easy and accessible to all Australians, including the 1.2 million Australians with profound or severely limiting disabilities[5]. Because of this a person can vote in a number of ways without attending a polling station on election day. These include voting by post, voting early, voting at an overseas voting centre (most Australian embassies and missions), voting at a mobile polling station, voting by telephone or voting with the assistance of a trusted friend, relative or AEC official. The current methods, though sometimes cumbersome, have resulted in 92-97% voter turnout for all elections since 1928[6]. Whether the extra 3-8% would utilise internet voting if available, is questionable. Enabling disabled Australians to vote is important. As is increasing voter turnout.

[5] Australian Bureau of Statistics Census 2009, freely available here: http://www.abs.gov.au/ausstats/abs@.nsf/Latestproducts/4430.0Main%20Features22009?opendocument&tabname=Summary&prodno=4430.0&issue=2009&num=&view=

[6] http://www.aec.gov.au/Elections/australian_electoral_history/Voter_Turnout.htm, accessed 2013-03-13

But there are ways of achieving this without compromising the security of our most fundamental expression of democracy.

Our interactions are increasingly moving online. The internet is an empowering technology. Surveillance concerns aside, email and internet banking have vastly increased the speed and efficiency of commerce and communication. Technology has significant potential to help our lives in myriad ways. But voting is different– it is the only direct method of influencing the laws under which we're governed. The verification of internet voting is significantly different to internet commerce. When we buy something online, we see the money leave our account and get sent the good. If either we find something amiss, we can check our bank accounts or take up the matter with an ombudsman. With voting, we would see our vote leave and then see the final tally. Any verification requires intricate knowledge of programming, and even then cannot guarantee final validity. A single mistrusted vote compromises the trust in the whole election: was my vote changed, or yours?

Computer systems can be hacked. During the past decade, the institutions that have been compromised include government departments, multinational companies, intelligence agencies and media organisations. The incentive to hack a national election is exceptionally high. Any electronic voting system will, by definition, have to send data electronically across the country, store it securely and process the information into readable results. Each step along the process is vulnerable to attack. From the very use of electronic voting stations[7], excellently parodied by The Simpsons[8], to the platforms themselves, as shown by Dr Halderman and his team. One small mistake in a line of code written by a public servant can have drastic consequences about which we might never be aware. With electronic voting, it will only be a matter of time before an election isn't decided by voter intentions, but by international terrorists, or a despotic government of the day, or by a pimply faced 15 year old drinking coke in his bedroom hacking the Australian Electoral Commission in between World of Warcraft raids.

These aren't hypothetical considerations. Electronic voting is happening now in various jurisdictions around the world, including Australia. Live trials of electronic voting are ongoing and expanding. In 2010 the NSW Government passed legislation for *iVote*, a trial remote electronic voting system that cast 47,000 votes over the internet in the 2011 State Election. 900 votes were cast for the seat of Balmain which was ultimately decided by a margin of hundreds of votes[9]. The system was not open-souce nor publicly verifiable. Switzerland and Estonia currently employ remote electronic voting on a widescale national level; all advanced countries are considering it. A few have chosen not to follow e-voting after community consultation, Sweden and New Zealand and two examples, others have halted implantation following large-scale trials – this has happened in the UK, USA and The Netherlands. Australia should follow suit.

The dangers are known to the Australian Department of Parliamentary Services[10], compiled in a report by Brenton Holmes. Whilst detailed and comprehensive, the report, written with typical public service restraint, is neither not.

These arguments don't depend on technological capability nor software structure. There are serious flaws in systems currently in use, but it's foreseeable that many of these technological issues will be ironed out. Systems currently exist that are open source, verifiable and secure to all possible known

[7] Examining touchscreen vote flipping, http://www.youtube.com/watch?v=0Q9NSVUu8nk

[8] Homer Simpson tries to vote for Obama, 1.5 minute clip here: http://www.youtube.com/watch?v=1aBaX9GPSaQ

[9] Teague and Wen, The Converstion, published online 2011-04-05, http://theconversation.com/can-we-trust-online-voting-616, accessed 2013-04-14

[10] Brenton Holmes, Australian Parliamentary Library, accessed 2013-04-14, http://www.aph.gov.au/About_Parliament/Parliamentary_Departments/Parliamentary_Library/pubs/BN/2012-2013/EVoting

attacks. But none can compensate for the inherent ‘brittleness’ in such systems that Drs Halderman and Jefferson warn us of. None provide for the scrutineering of votes by a member of the general public. For the benefits of vote-counting taking 3 minutes instead of 3 hours and for the possibility of increasing voter turnout by 3%, the dangers of electronic voting are not worth it. Not now, nor for the foreseeable future. When we complain that our politicians are robotic and inhuman, maybe one day our complaints will be more accurate than we realise.