



VOTE FOR ONE CANDIDATE ONLY

1  
2  
3

**TUCKER**  
Malcolm Tucker  
The Labour Party Candidate



**GLADSTONE**  
William Ewart Gladstone  
Liberal Democrat Party Candidate



**B'STARD**  
Alan Beresford B'Stard  
The Conservative Party Candidate



SAMSUNG  
12:03

# eLECTION

# 2015

---

## Why can't we vote online?

---

You can do pretty much anything online these days, but voting has barely changed since the 19th century. As Britain prepares to go to the polls again, **Simon Handby** considers the case for casting your ballot online

**I**t's unlikely to have escaped your notice that on 7th May we'll be heading to the polls for the 2015 general election. The issues, personalities and policies may (arguably) change, but the way we vote in the UK certainly hasn't. We'll be marking our choice on the ballot paper in the usual way – yet these days we can do everything else online. So why aren't we choosing governments from the comfort of our laptops? In this feature we look at the technology of voting, and at the changes technology is bringing to elections and politics.

### Spoiled paper

For most of us, it won't be a great hardship to swing by a polling station on 7th May, but when we get there we'll be presented with a scenario that would be recognisable to our great-grandparents: after identifying ourselves we're presented with a ballot paper on which we mark a cross, then we fold it, post it in a ballot box and go home to await the result. Ballot boxes are collected and transported to a central counting location, where volunteers and officials sort and count their contents by hand; a constituency's result isn't usually known until at least a couple of hours after the poll has closed.

In an age when we can provide detailed financial records to the taxman via an online form, or transfer thousands of pounds safely with a mobile app, our paper-based, labour-intensive voting system looks increasingly out of date; indeed, it was introduced with the Ballot Act of 1872. However, before we write it off, it's important to consider its strengths. A free and fair election requires that only those entitled to vote should do so, that they should each do so only once, and that they should be able to do so in privacy and without fear of coercion or reprisals.

Currently, in theory at least, each voter proves they're eligible to vote by identifying themselves, and their name is crossed off the list of voters so they can vote only once. Although a record is kept linking each voter's elector number to their ballot paper number, it's sealed at the close of polls and can't be





It may be dated, but a paper ballot is effective at protecting the privacy of our vote

Reproduced with kind permissions of the Electoral Commission

↑ If it's good enough for the bank...

opened without a court order, preserving the anonymity of our votes unless the election's validity is challenged. As such, we need have no fear of reprisals. By splitting the vote across multiple polling stations, each manned by multiple officials and using multiple ballot boxes, the potential impact of any accident or subterfuge is comparatively limited.

However, concerns about the accessibility of voting and falling voter turnout has led to a relaxing of the rules on proxy and postal voting: since 2001, anyone can apply for a postal vote without giving a reason. Unfortunately, it soon emerged that postal voting in particular was subject to malpractice: in 2005, five men were found guilty of a large-scale fraud involving thousands of postal ballots, in the Birmingham local elections of June 2004.

While changes to the system have subsequently made it more secure, remaining criticisms include that it is far too easy to create fake or duplicated entries on the electoral roll, a practice known as 'roll stuffing'.

### The technology problem

It's easy to assume that modern technology would provide the perfect answer. An ideal electronic system would certainly bring advantages: the electorate could vote from a polling station, but also from home, work, or anywhere they could get a data connection. Results could be tabulated and calculated automatically and centrally, providing a near-instant result and reducing the logistics and cost of an election. With fewer staffing and location concerns, polls could stay open longer, increasing turnout.

But implementing such a system is far from straightforward, and getting it wrong could have grave consequences.

electronic voting within the polling station, present two quite different challenges. Heather thinks the greatest challenge lies in internet voting, which poses a different problem to, say, the secure exchange of information with your bank: "When you do your online banking, you're trying to protect information that's going between you and the bank. But everything you know about your bank account, the bank also knows: there's no secret between you and the bank."

Heather contrasted this with internet voting: "I'm not interested in getting my vote to the returning officer so that only me and the returning officer know how I voted. What I want to do is to get my vote into the system so that it can be included in the count without anybody knowing how I voted."

According to Heather, this means a voting system can't just encrypt your vote, send it to a returning officer for decryption and trust they won't share it with a third party. Certainly, without any attempt to decouple the identity of the voter from the vote they cast, voters could be open to reprisals.

Some kind of shuffling of an electronic vote is needed, then, much as ballot papers become shuffled in the ballot box before they're counted. It's here that we should introduce another requirement of the ideal voting system: each voter should be able to verify that

## A successful hack on an electronic system could change the result of a general election

While many consider our current voting arrangements too susceptible to fraud, a successful hack on an electronic system allows a far more insidious and widespread manipulation of the poll; in the worst case, changing the result of an entire general election.

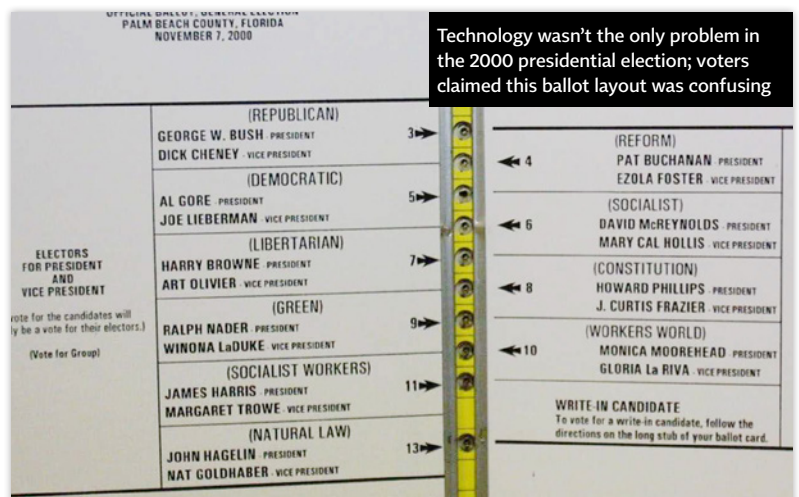
We spoke to Dr James Heather, a computer security expert with a particular interest in electoral security, who stressed that internet voting, and

## REGISTER TO VOTE



In 2014, the government scrapped the previous 'head of the household' voter registration system, where a single respondent would register and confirm all those living at an address who were eligible to vote. It's now the responsibility of individuals to ensure their name appears on the electoral register, a change which critics say has led to a drop in registration, particularly among first-time voters.

If you're unsure whether you're registered to vote, the first step is to check with your local council's electoral services department, which is responsible for maintaining the register. If you're not registered, or if you want to apply for a postal, proxy or overseas vote, visit [www.aboutmyvote.co.uk](http://www.aboutmyvote.co.uk) urgently.



their vote has been correctly received and counted, and potentially change their vote up until the close of polls.

### Unhappy returns

With the perfect electronic system in mind, it's instructive to look at earlier attempts at electronic voting and vote counting around the world. The most notorious example is the 2000 US presidential election in Florida, which put George W Bush in the White House. Various post-election studies revealed multiple issues with the state's vote, affecting both candidates, including poorly designed ballot papers and badly written instructions to voters. However, two of the biggest problems arose from automated voting machines, which produced the infamous 'hanging chads', and counting machines that mis-categorised or incorrectly rejected thousands of votes.

Concerns have since been raised over electronic voting machines, which record voter intent through either push-button or touchscreen interfaces. The US has used such machines quite extensively, but in 2009 the Argonne National Laboratory in Illinois demonstrated a successful, apparently simple man-in-the-middle attack on a Sequoia AVC Advantage e-voting system, as used in New Jersey. In 2011 the same team demonstrated similar vulnerabilities in a Diebold AccuVote touchscreen system. In both, votes for one option appeared to have been registered correctly, but were manipulated so that the machine in fact recorded an alternative option.

In Ireland, experiments with electronic voting were disastrous. In the 2002 general election, electronic systems made by Dutch firm Nedap underwent trial in three constituencies, with a view to rolling similar technology out nationwide. However, a subsequent Department of Environment report raised concerns that the integrity of the ballot couldn't be guaranteed with the equipment and controls in place, and that voters could be duped into voting for the wrong candidates if a fake ballot was simply taped over the machines' front panels.

In 2006, Dutch hackers claimed to have reprogrammed a Nedap ES3B voting machine – used in Germany, France and the Netherlands – such that “anyone, when given brief access to the [device] at any time before the election, can gain complete and virtually undetectable control over the election results”. Also of concern, they claimed that radio emanations from an unmodified machine could be read to reveal the vote cast. In 2012, after many years in storage, Ireland's voting

## BLANK CANVAS

### How technology helps politicians engage



Many of us will have been visited by party workers, councillors or even MPs in the run-up to an election, as they attempt to gauge support and mobilise voters in key constituencies. This year will be no different, but such face-to-face canvassing is part of a wider effort, one in which parties hope that the latest tools and platforms will give them an advantage.

These days, social platforms such as Twitter and Facebook are a must for politicians seeking to engage with the electorate, with central party offices typically also using YouTube, Google+ and Instagram. We contacted Labour, the Conservatives, the Liberal Democrats, the Green Party and UKIP to ask for details of the teams manning such accounts, and whether – as is common with larger businesses – they were supported by external, digital agencies. All declined to comment.

We were also keen to discuss the use of software for tracking and mobilising support, such as NationBuilder – an internet community-building service cited by US Democratic Party members as their most important advantage over Republicans in the 2012 US presidential election. As Willard Foxton, blogging for the *Telegraph*, explains: “[NationBuilder] doesn't stop the grind of an election campaign – the door knocks, the rallies, the speeches – but what it does is link online and offline, making sure online campaigning leads to targeted offline follow-up.”

The software allows campaigners to build detailed profiles of potential supporters and use these to target resources in the run-up to the vote. The Scottish National Party trialled the software in its Scottish Parliamentary election victory of 2011, and UKIP, Labour and the Liberal Democrats are using it now, but no-one we contacted would discuss exactly how.

A Labour Party spokesperson did explain that the party's aim was to engage people through social media, “rather than to broadcast at them”, and that “we try to bring political issues to life by creating personalised digital experiences that engage users”.

“Digital campaigning doesn't exist in a silo,” they added. “Everything we do is focused on winning votes in the real world, by encouraging supporters to take action as a result of our content.”



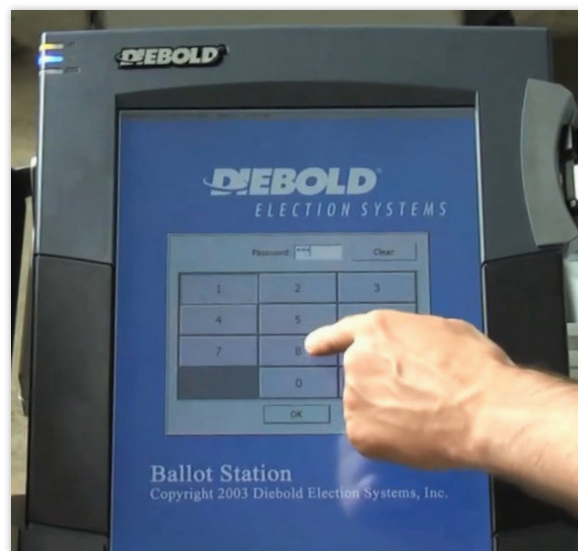
↑ Not the kind of engagement that the Labour Party was looking for from its digital presence

machines were scrapped. The project had cost an estimated €55 million.

### Trial and error

Nothing so dramatic has happened in the UK, but attempts to modernise the way we vote have been ongoing for a while. In addition to the 2001 changes to postal and proxy voting, the government began encouraging local authorities to run pilots of alternative voting methods, including electronic voting. Of participating authorities, Sheffield City Council and Swindon Borough Council have undertaken the

↓ The Argonne National Laboratory released a video demonstrating a successful hack of a Diebold electronic voting machine



most systematic pilots, at local elections in 2002, 2003 and 2007.

Announcing the 2003 trials, then local government minister Nick Raynsford claimed the scale of the 2002 pilots was such that “the UK is rightly regarded as being among the pioneers of electoral modernisation”. In the 2015 general election, however, there will be no electronic voting, so what exactly went wrong?

In Raynsford's defence, he made clear that new technology would proceed further only if the government was satisfied it was secure and robust. In 2007, the Electoral Commission – which oversees elections in the UK – recommended electronic voting should be halted on the grounds that security and implementation would need to be improved before it could move forward. While acknowledging the commission had learned much from pilots, its then chief Peter Wardle said: “We do not see any merit in continuing with small-scale, piecemeal piloting where similar innovations are explored without sufficient planning and implementation time, and in the absence of any clear direction, or likelihood of new insights.”



According to some, it's a good thing we haven't moved forward. Dr Stuart Wilks-Heeg, head of politics at the University of Liverpool, explained that, since 2007, "evidence of profound problems with the security of e-voting has emerged internationally".

"For example, in 2013, hackers showed how it was possible to access Geneva's e-voting system for referendums to change a 'yes' vote to a 'no', and vice versa. Also in 2013, French journalists were able to cast fraudulent votes in an open primary to select the [opposition] UMP's candidate for the Paris mayoral election."

Such interference, together with the aforementioned man-in-the-middle attacks, are deeply worrying, but Dr Wilks-Heeg raises a more ominous threat: that a foreign power could launch an orchestrated attack on a vote through a central weaknesses in the system, or via malware.

### Where there's a will

Against this backdrop, it's perhaps understandable if the enthusiasm of Tony Blair's Labour government for "an e-enabled general election some time after 2006" has evaporated somewhat. The loss of the 2011 referendum on the Alternative Vote dampened the present government's enthusiasm for reform of our electoral mechanism, even if – as several experts pointed out – reform of the electoral system and of electoral technology are two different things.

However, the will to implement electronic voting does appear to be building again. In November 2013, the Speaker of the House of Commons,



↑ In Smartmatic's Belgian system, electronic machines produce a paper ballot slip

John Bercow, set up of the Commission on Digital Democracy (CDD), which released its final report in January 2015. It recommended that by 2020, not only should "secure online voting... be an option for all voters", but that an "interactive and digital" parliament should experiment with ways for the public to put questions to ministers and contribute to the law-making process.

Given the current lack of momentum, it seems unrealistic to expect that an internet voting system could be implemented by the time of the next general election. Dr Wilks-Heeg spoke of a consensus among experts that it would take at least 10 years to ensure that internet voting was secure from fraud or hacking. There are many companies offering electronic voting systems for the polling station, but Dr James Heather cautioned that "[there is a distinction] between what's commercially available,

and what has been designed and subjected to some academic rigour".

For their part, the makers of electronic voting machines argue that security has improved hugely since the last UK trials. Smartmatic, a London-based voting systems company, told us its voting platform "was designed, from the beginning, by taking into account all possible physical and electronic threats a voting system might be exposed to". For example, configuration data and votes are encrypted within the voting machine so they can't be read or modified, which ought to rule out a man-in-the-middle attack.

### Belgian waffle

Smartmatic is keen to highlight its role since 2012 in parliamentary, local and European elections in three regions of Belgium. In that system, voters arriving at the polling station are identified and issued with a smartcard that will enable

## A TIDY EXIT Why we know the result before it's announced



For hours after an election we rely on exit polls, which are often wide of the mark – notably in 1992, when a hung parliament was predicted ahead of a Conservative majority. To address such inaccuracies, from 2005 the BBC and ITV agreed to pool their data for a single exit poll.

Since then, you might as well have gone to bed at the close of voting, with the 2005 exit poll correctly predicting a 66-seat Labour majority, well before a single constituency had declared. In 2010, the poll correctly predicted a hung parliament with 307 seats for the Tories; in the event they won 306. Many commentators raised eyebrows at its forecast of a poor 59 seats for the Liberal Democrats, given their strong position in opinion polls immediately before the vote. In the event, however, they won just 57 seats.

We spoke to John Curtice of the University of Strathclyde and head of the team responsible for the poll, who explained its data gathering is conducted at around 130 locations by means of a paper ballot and ballot boxes, similar to the actual vote. Researchers count the results, then forward it to the team for subsequent modelling.

Curtice poured cold water on our suggestion that the poll's recent accuracy might be down to improving technology, explaining instead that as much as possible, samples are taken at consistent polling locations between elections. With a record of how a

location's previous exit poll and results compare, it's possible to make a more accurate estimate of what the latest poll represents. From that, the team can derive a more accurate estimate of what the outcome might be across the country.

Curtice explained that the accuracy of the 2010 prediction for the Lib Dems was just down to the data, or "simply a case of asking people what they did and not getting many more people [voting Lib Dem] than five years previously". Accurate data was behind the Tory prediction, too, but in this case the team also spotted that Labour was performing better than anticipated in Scotland and in areas with a high ethnic minority population, and used this to reduce the estimate of overall Conservative seats.

Poll calculations are probabilistic, which is to say that the team calculates the likelihood of the possible outcomes in each polled location, and creates a nationwide model using these. Curtice explained that in the 2015 election this approach would be vital in predicting the UKIP vote: "We'll get an awful lot of seats where UKIP might have a five or 10 per cent chance of winning, and as a result of that, somewhere or other UKIP are going to pick up a seat. Don't ask us which one it is – it could be one of 10 possible places – but we suspect that somewhere or other they'll strike lucky."

them to activate a standalone touchscreen voting machine. Once they have made their selections, the machine prints a paper record of the vote, containing all the selections in plain text together with a QR code representing them. Voters must post this in an electronic ballot box, which stores the paper vote, but also reads the QR code and transfers the data to the central 'president machine'. Votes are encrypted, stored on two USB drives, and the voter returns their de-activated smartcard before leaving.

Smartmatic says its solution was chosen after a two-year process involving authorities, universities and PricewaterhouseCoopers. Among the system's advantages is that the identification of voters is achieved separately from their vote: the smartcard serves only to authorise a vote, rather than identify the voter to the voting machine. There's also a paper trail to assist in auditing. However, the system doesn't allow voters to verify that their vote has been received and counted.

Smartmatic also offers the example of Estonia, where since 2005 the electorate has been able to vote via the internet in a system originally developed by the Estonian company Cybernetica, and the Estonian National Electoral Commission (VVK). In that year only 9,317 people chose to vote online, but in the most recent Parliamentary elections in March, this had risen to more than 176,000 people – 30% of all votes cast.

In the Estonian system, voters have seven days in which to cast a vote online. In order to vote, they must install a digitally signed app from the VVK website, then verify their identity using either their digital ID card – a biometric card issued to Estonians since 2002 – or with a security code sent to their mobile phone. Once identified, the voter can make their selections from an electronic ballot,



Andrus Ansip, former Estonian prime minister, casts his vote online

and must verify their identity again before submitting it.

### Let me see your ID

We asked Smartmatic how the Estonian system ensures that a vote is separated from a citizen's identity. Michael Summers, the company's internet voting director, told us: "The principle is rooted in the double-envelope system used for traditional postal voting in some countries. An inner 'virtual envelope' contains the encrypted vote, and the outer virtual envelope is digitally signed. Before counting occurs, both envelopes are separated.

"The [outer] envelope with personal data is discarded after its mission of conferring the eligibility of the voter and authenticity of the vote. The [inner envelope] is sent to the digital ballot box. The encrypted, anonymised votes are then cryptographically 'shuffled' to randomise the casting sequence, and are then transferred to a 'clean', air-gapped counting server, where they are decrypted by a quorum of election officials."

Despite the apparent security of this approach, however, in 2014 a team at the University of Michigan conducted what it described as an independent evaluation of the system, concluding that it had 'serious design weaknesses... exacerbated by weak operational management' and that its use should be discontinued. In response, VVK stated that the system had been used in six elections without "a single incident [that had] influenced the outcome", but the researchers disagreed. You can read further discussion about the system at [tinyurl.com/shopperestonia](http://tinyurl.com/shopperestonia).

What's certain is that, like other remote voting arrangements including postal voting, Estonia's system is susceptible to small-scale,

unsophisticated attacks. In essence, as Dr James Heather puts it: "Whatever security measures you have for encrypting things, there's just no way of knowing that there isn't somebody standing behind me with a baseball bat while I'm voting."

### Vote of confidence


In the internet age the UK's paper-based, labour-intensive elections are an anachronism, but it appears this isn't just down to a lack of political will. Implementing secure systems that prevent fraud yet protect the anonymity of our vote is a huge and expensive undertaking, and questions remain about even the most successful implementations to date worldwide.

In addition to these concerns, there's scant evidence to support arguments often raised in favour of electronic voting, and internet voting in particular. Most significantly, many studies appear to suggest that the

## There's scant evidence to support arguments often raised in favour of electronic voting

availability of internet voting results only in a small improvement in turnout; in most cases, people who voted online say that they would have voted by other means if necessary.

Analysing turnout after the increased availability of postal votes in the 2005 general election, Professor John Curtice (see 'A Tidy Exit', opposite) wrote: "Not even the prospect of [avoiding] the journey to the polling station enticed many voters to exercise their franchise."

He added: "Turnout depends not on giving people a choice about how to vote, but rather on what they are voting about." 

British democracy has come a long way since the Palace of Westminster was finished in 1870, but we think it can come further

