The Foundation for Information Policy Research

Response to

The Speaker’s Commission on Digital Democracy

The Foundation for Information Policy Research (FIPR) is an independent body that studies the interaction between information technology and society. Its goal is to identify technical developments with significant social impact, commission and undertake research into public policy alternatives, and promote public understanding and dialogue between technologists and policy-makers in the UK and Europe.

FIPR has the following comments to make in response to the questions asked by the Speaker’s Commission on Digital Democracy on electronic voting.

1. Allowing votes to be cast remotely from PCs and phones may seem an attractive way to make voting easier and increase turnout – goals that everyone can support.
2. Electronic voting has for some years been used routinely by the Electoral Reform Society and others for many low-stakes elections, such as to the leadership of professional bodies.
3. However this technology still has very significant issues with security, privacy, coercion resistance, auditability and comprehensibility, which preclude its use in high-stakes contests where capable and well-resourced actors (political parties, lobby groups and even foreign governments) may have an incentive to manipulate the system.
4. Technical security issues arise from the insecurity of existing consumer systems and Internet infrastructure. Most personal computers and smartphones are wide open to compromise by malicious software, with perhaps 5% of PCs infected with malware at any time. Once machines are compromised, their owners have little control over what their devices are doing on their behalf. Bulk access to compromised machines is bought and sold on the black market by spammers, bank fraud gangs and other wrongdoers (including nation state actors) who could easily use such capabilites to change the outcome of a close-fought UK election (or referendum) by producing a swing of a few percent in key marginal constituencies.
5. The strong privacy requirement for ballots makes security even harder. The security of online banking, e-commerce, and other Internet-based systems rests on the availability of information about the transactions to multiple parties, who can check and if necessary reverse them. Thus a bank customer whose PC is infected with the Zeus malware, which makes unauthorised transactions on his behalf, may be saved when the bank notices and blocks the transactions it tries to make, and if not she can be made whole by a refund after the fraud is discovered. This is much more difficult with votes, as it is difficult to combine privacy and auditability.
6. This is related to the coercion resistance requirement. It must be difficult for a voter to prove which way he voted, else he might be bribed or threatened. In current systems we achieve this by giving voters a ballot paper in the polling station where the ballot box is located and from which political organisers are excluded. (Even this is not perfect; in

chain voting, an organiser gives a voter a completed ballot paper before he goes into the polling station, and he's expected to put this in the ballot box and bring out a fresh one to the organiser in order to claim his bribe.)

7. A move to Internet voting, in which people were emailed a voter code and then used this at a ballot website (as happens with low-stakes online elections today), would leave voters wide open to bribery, intimidation and coercion. They would not just be vulnerable to ruthless political organisers, as in the chain voting case, but to family members and others. There have been many suggestions as to how online voting might be made more coercion resistant, such as allowing people to vote several times with only their last vote counting, but none are perfect.
8. Coercion resistance is also in tension with auditability, since an unexpected result (or a close one) can lead to a legal challenge, whereupon the result must be justified. Attempts to design elections that are both coercion-resistant and auditable seem to lead inevitably to complex schemes involving fancy ballot papers or software that does complicated cryptographic mathematics. Again, none of these is perfect, and few of them are even comprehensible to ordinary voters (or politicians) who do not have graduate-level training in security engineering.
9. An election system must be comprehensible in order to gain and hold public trust. Simply saying "GCHQ's mathematicians have determined that this scheme is sound, but we can't tell you the details for security reasons; trust us" is a non-starter. Conspiracy theorists will have a field day, and minority parties will play up their fears in order to discredit the election and even undermine democracy itself.
10. The current system, of paper ballots counted in bundles on tables in town halls in front of observers from the competing candidates and parties, achieves a remarkably good trade-off between security, privacy, coercion-resistance, auditability and comprehensibility. No online system of which we are aware comes even remotely close.
11. These factors have been extensively discussed in expert reports over the last decade. We can recommend two, whose conclusions remain valid:

    a. David Jefferson, Aviel D. Rubin, Barbara Simons, and David Wagner. A Security Analysis of the Secure Electronic Registration and Voting Experiment (SERVE). Report to the Department of Defense (DoD) Federal Voting Assistance Program (FVAP), January 20, 2004. <http://www.cs.berkeley.edu/~daw/papers/servereport.pdf>

    b. Jason Kitcat. Electronic Voting: A challenge to democracy? Open Rights Group briefing paper, January 2007. <https://www.openrightsgroup.org/wp-content/uploads/org-evoting-briefing-pack-final.pdf>

12. These reports also tackle some of your other questions – for example, concluding that there is little evidence that online voting has so far had a significant impact on turnout. Rather, voters are encouraged when they feel they have a genuine choice and a chance to make a difference – the recent Scottish referendum being a prime example.
13. There are issues about disenfranchising voters that do not have access to personal computers or smartphones, or adequate broadband. The Office of National Statistics found that in 2014, 13% of British adults have never used the Internet

<http://www.ons.gov.uk/ons/rel/rdit2/internet-access---households-and-individuals/2014/stb-ia-2014.html#tab-Computer-and-Internet-Use>, while Ofcom's Communications Market Report 2014 <http://stakeholders.ofcom.org.uk/binaries/research/cmr/cmr14/2014_UK_CMR.pdf> (p.9) states that 8% of UK premises' broadband connections are still less than a basic 2Mb/s. It may be worth bearing in mind that Glasgow, which seemed disenchanted with the UK in the Scottish referendum, has the lowest broadband use of any city in Europe.

14. A recent investigation of Estonia's e-voting system, conducted by an expert team of European and American security researchers and election auditors, concluded:

> *[T]here are multiple ways that state-level attackers, sophisticated online criminals, or dishonest insiders could successfully attack the Estonian I-voting system. Such an attacker could plausibly change votes, compromise the secret ballot, disrupt elections, or cast doubt on the integrity of results. These problems are difficult to mitigate, because they stem from basic architectural choices and fundamental limitations on the security and transparency that can be provided by procedural controls. For these reasons, we recommend that Estonia discontinue the I-voting system.*

(Drew Springall, Travis Finkenauer, Zakir Durumeric, Jason Kitcat, Harri Hursti, Margaret MacAlpine, and J. Alex Halderman. Security Analysis of the Estonian Internet Voting System. Proceedings of the 21st ACM Conference on Computer and Communications Security (CCS '14), November 2014 <https://estoniaevoting.org/findings/paper/>)

15. In our view, the adoption of online voting technology would present extremely grave challenges to the integrity of UK elections, and risk disadvantaging significant sections of the population., which would present a real danger of undermining public confidence in democracy rather than strengthening it as the Commission rightly seeks to do.
16. Finally, people who oppose the use of new technology for well-established activities are sometimes accused of being Luddites and of letting their ignorance stand in the way of perfectly acceptable change. In the case of e-voting, we believe that the more familiar people are with the technology, the more they understand the very substantial risks that it poses to the democratic process. It is ignorance that leads people to suppose that e-voting is risk-free and desirable; and it is technical experts such as ourselves (and our colleagues whose carefully-argued papers we have cited) who are cautioning against embracing e-voting for the foreseeable future.

Ross Anderson FRS FREng
Professor of Security Engineering
Computer Laboratory
University of Cambridge

Ian Brown
Professor of Information Security and Privacy
Oxford Internet Institute
University of Oxford

September 23rd 2014