Should We Vote Online?

Martyn Thomas CBE FREng
Livery Company Professor of Information Technology
Gresham College

Principles of Democratic Election
Venice Commission

- **universal:** in principle, all humans have the right to vote and to stand as a candidate
  (may depend on age, nationality, residence …)

- **equal:** voting rights. number of votes, opportunity to stand, access to media, public funding …

- **free:** state authorities must be neutral. Voting must be simple, secure, protected from coercion and fraud.

- **secret:** secret voting is a right and a duty. Must be individual. No family voting or coercion. Disclosed ballots must not count. No publication of lists of who actually voted (as abstention is political)

- **direct:** One chamber of the national parliament, lesser legislative bodies and local councils must be directly elected every 5 years or less.

UK secret ballot since 1872, although the *corresponding number list* was introduced to combat fraud. Any abuse is a criminal offence.

Democracy Depends on Elections
– and low participation weakens it

In the UK

- Most citizens over 18 are entitled to register to vote in parliamentary elections. **47 million people**

- About **89%** of those eligible do **register**

- About **68%** of those registered **actually voted** in the last General Election. That's only **60% of the electorate.**

- Participation is far lower in local elections.

"*a trusted election process is one that works, can be shown to have worked after the election has been held, can be shown to have not been manipulated and to have not led to a large number of mistaken or lost votes, and can be shown to reflect the intent of the voters.*"

– **US National Academies report**: *Asking the Right Questions About Electronic Voting*

Risks and Threats
to a fair election

- Fraudulent registration

- Excluding some (groups of) voters

- Vote stealing by impersonation

- Coercion

- Vote selling

- Violations of the secret ballot

- Prevention of voting by some (groups of) voters

- Incorrect counting

- Anything that causes the electorate to lose confidence in the fairness of the election

The Current UK Voting System
simplified - see the transcript for more details

- Register at age 16 (Eng, Wales, NI) or 14 (Scotland)

- Vote at age 18 (Eng, Wales, NI) or 16 (Scotland)

  - Vote in person at a polling station, or

  - Vote by post, or

  - Vote by proxy.

Postal Voting

- Anyone can apply to vote by post

- Very easy to understand…

- … but it has weaknesses.

In the 2004 Birmingham fraud case, about half of the votes for the winning candidates were said to be fraudulent

"The scale of fraud would disgrace a banana republic" said the election commissioner.

Postal voting is accepted - a valid benchmark for on-line voting?

Fraud

In March 2008, passing initial judgement on the Slough case, Richard Mawrey QC, again acting as election commissioner commented that: 'to ignore the probability that [fraud] is widespread, particularly in local elections, is a policy that even an ostrich would despise.'

Figure One: Persons found guilty of electoral malpractice in the UK, 2000-2010, by year of election

Source: democraticaudit.com
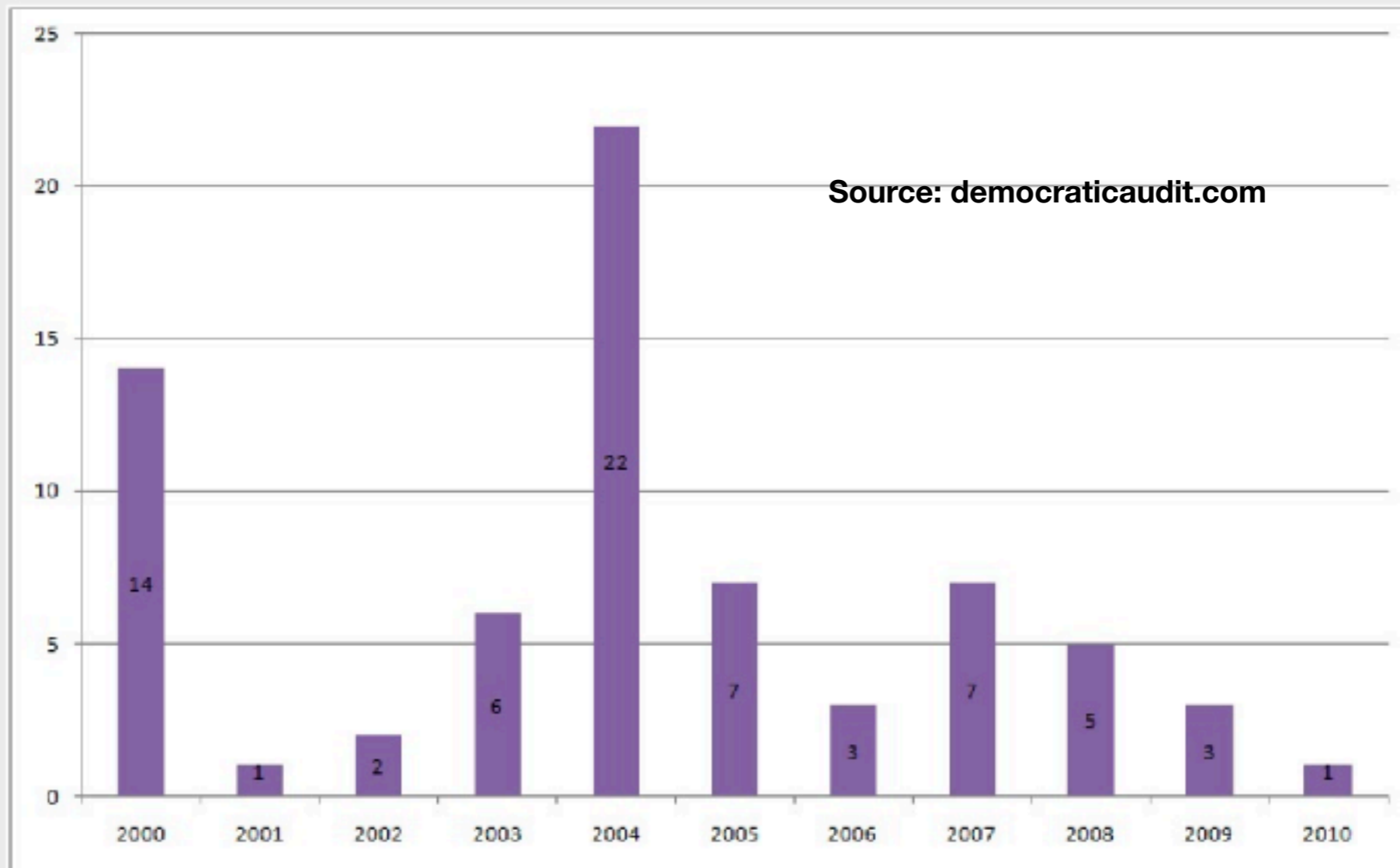
Note: Statistics are based on known cases, as of 22 March 2011. A number of allegations reported to police in 2010 were still under investigation at this time.

Individual Electoral Registration
– introduced to reduce the opportunities for fraud

- From December 2015, voter registration changed from Household Registration to Individual Registration.

- Individuals have to provide their Date of Birth and National Insurance Number (exceptionally, other ID)

- The ID is verified against the DWP database (or locally by Electoral Registration Officers).

Figure ES.2: Applications to register to vote under IER (10 June 2014 to 9 June 2016) - Digital (online) and paper form.
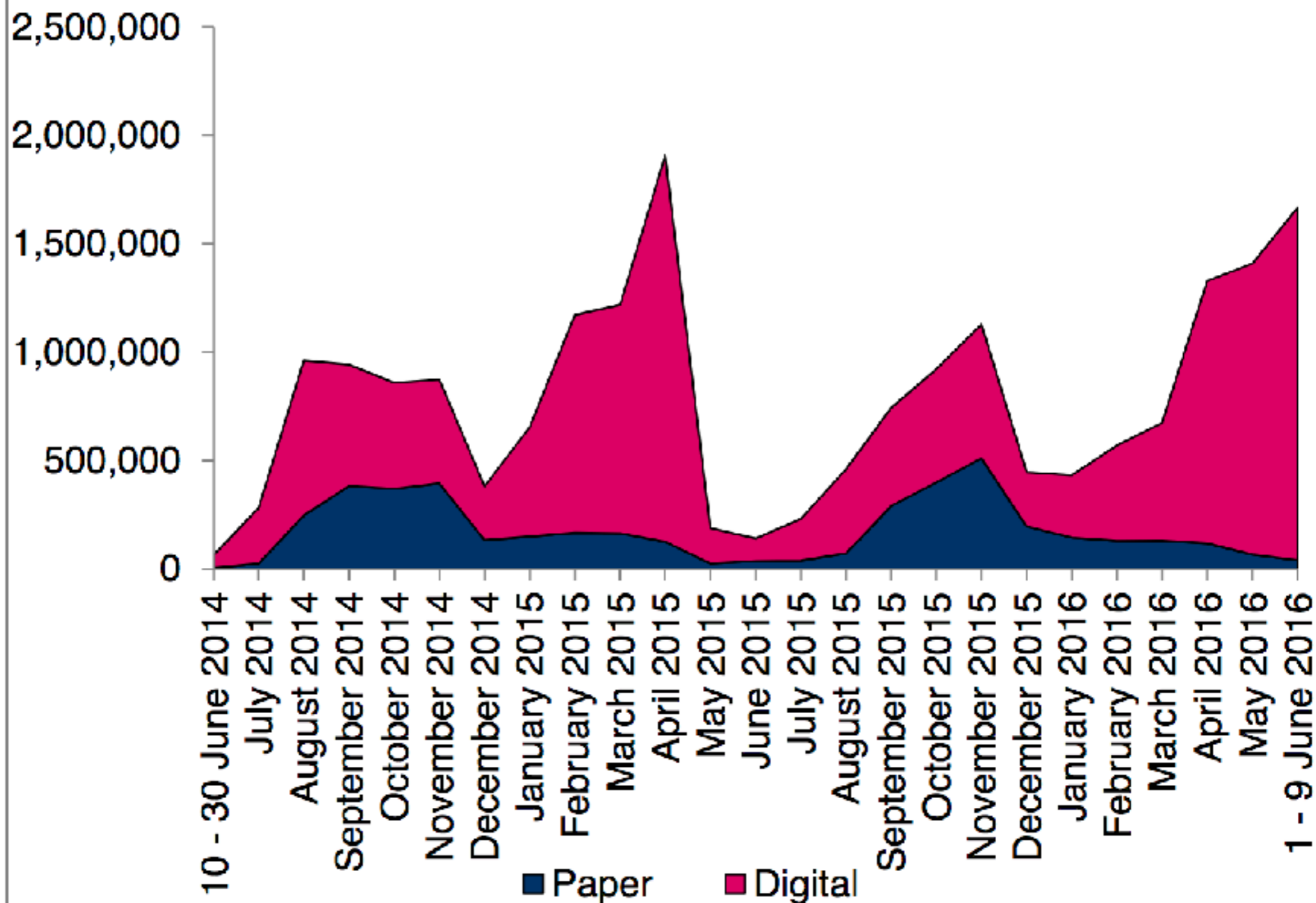
The deadline for registering to vote in EU Referendum was 9 June 2016.
Source: https://www.gov.uk/performance/register-to-vote.

Table ES.1: Accuracy and completeness of the register before and after the introduction of IER in Great Britain.

Quality indicator	Register	Pre-transition: Feb/Mar 2014	Post-transition: December 2015
Accuracy	Parliamentary	86%	91%
	Local government	87%	91%
Completeness	Parliamentary	86%	85%
	Local government	85%	84%

Accuracy: 'there are no false entries on the electoral registers'

Completeness: 'every person who is entitled to have an entry on an electoral register is registered'

Electronic Voting

- Electronic voting includes:

  - systems in polling station booths

  - temporary polling booths in supermarkets etc

  - online voting using a PC, tablet or smartphone

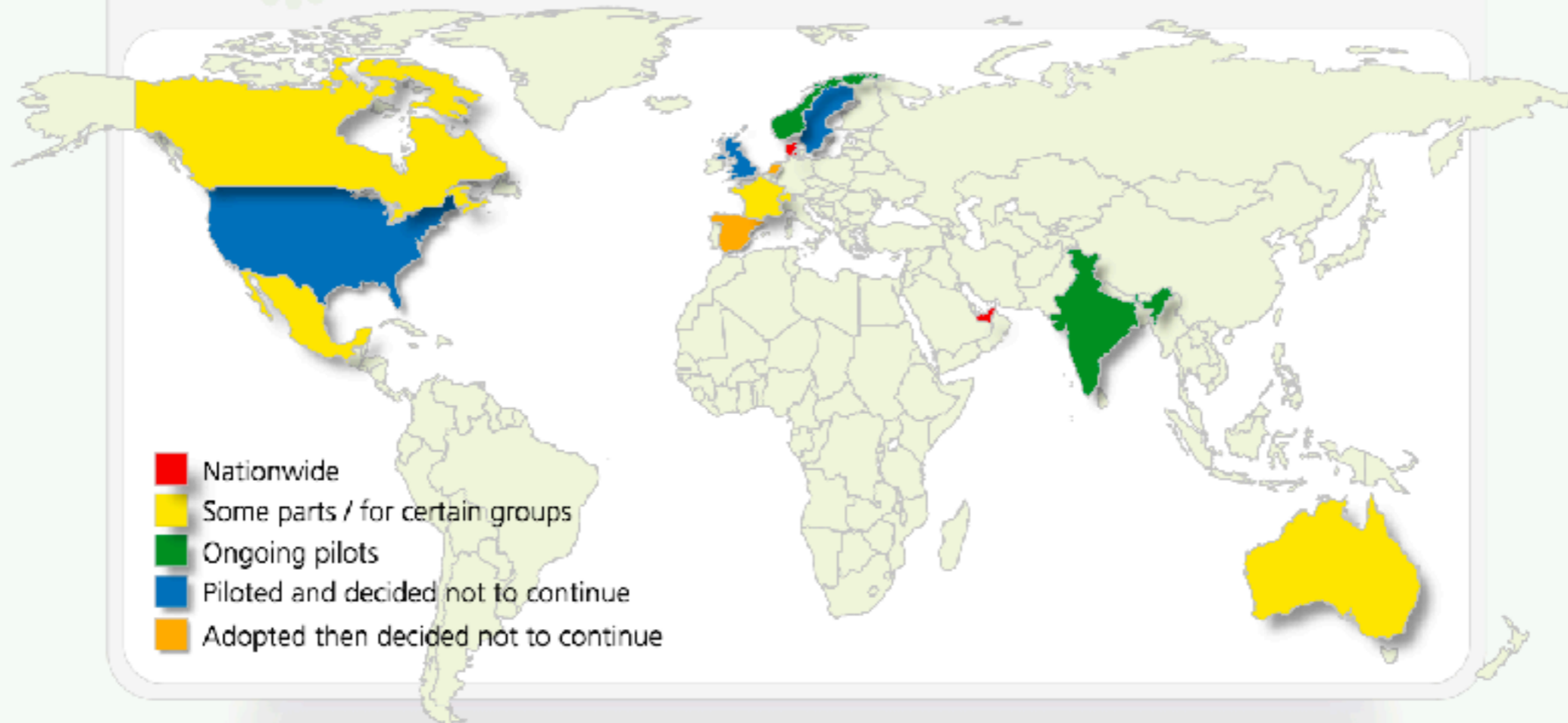- … probably combined with electronic vote counting

I focus on **online voting** in this lecture

UK Electronic Voting Trials

- May 2007 English local elections

  - 1.5 million voters in 18 local council areas

  - Various methods were trialled: online voting, telephone voting and mobile polling stations.

  - Despite a range of problems, the Electoral Commission said the trials proved successful but *"there remain issues with the security and transparency of the solutions and the capacity of local authorities to maintain control over elections"*

  They recommended no further e-voting until the problems were resolved.

Internet Voting around the World

Legend:
- **Red** — Nationwide
- **Yellow** — Some parts / for certain groups
- **Green** — Ongoing pilots
- **Blue** — Piloted and decided not to continue
- **Orange** — Adopted then decided not to continue

Estonia is the leading country for online government services including elections.

Estonian citizens all have cryptographic smart-cards that act as online identity cards

A group of international experts were invited to observe Estonia's 2013 municipal elections. They concluded that until there are fundamental advances in computer security, they do not believe the voting system can be made safe.

International and UK experience suggests that online voting does *not* increase the proportion of the electorate who actually vote.

Recent UK Consultations and Reports on Electoral Reform

- December 2014: the four UK Law Commissions consulted on electoral reform including online voting and in February 2016 they reported. They await a Government response.

- In January 2015 the Speaker of the House of Commons reported on his *Commission for Digital Democracy.*

- The Speaker's Commission said that people **expected** to be able to vote online, but highlighted security concerns, quoting the Open Right Group's summary:

"Voting is a uniquely difficult question for computer science: the system must verify your eligibility to vote; know whether you have already voted; and allow for audits and recounts. Yet it must always preserve your anonymity and privacy. Currently, there are no practical solutions to this highly complex problem and existing systems are unacceptably flawed."

They concluded that the security problems must be solved in time for online voting in 2020

In February 2018, the Scottish Government is in the process of consulting their electorate and the Welsh Government has just announced that there will be trials of online voting.

Important Properties of an Online Voting System

None of the Consultations Say!

1. It should be very difficult to register fake voters (and yet easy to register genuine voters).

This seems to have been achieved. The Electoral Commission are satisfied

2. The system should authenticate that the voter is registered to vote in this election.

This involves checking that the person who is voting is the same as the one who registered. Perhaps the Gov.UK Verify scheme would be enough.

Important Properties of an Online Voting System

3. No voter should be able to cast more valid votes than any other voter.

At simplest, no voter should be able to vote twice. In elections where there are several votes to be cast, the maximum number should be enforced.

Maybe multiple votes should be allowed but only the final vote counted? This could help defeat coercion and vote selling.

4. The voter should be able to check that their vote has been counted correctly.

This is important to give voters confidence in the system but hard to implement because a compromised system can give false evidence.

Important Properties of an Online Voting System

5. It should be possible to carry out an independent check that all valid votes have been counted and that the totals for each candidate are correct.

Re-counts are quite common in constituencies where the result is close. With paper ballots, the count can be repeated manually if necessary and supervised by the candidates. Devising an independent recount mechanism for online voting may not be possible.

6.It should not be possible to discover how a voter voted.

This is fundamental to the secret ballot. As explained earlier, the current paper ballot process includes the "corresponding number system" to allow a court to investigate a claim of fraud, with legal sanctions if the system is abused. Different mechanisms would need to be invented to combat the different threats of fraud that online voting would introduce

Important Properties of an Online Voting System

7. It should not be possible to discover whether or not an identifiable voter voted at all.

In some foreseeable circumstances, abstention in a ballot may be a significant political statement. In designing online voting system, it will be necessary to decide whether or not this is a necessary requirement.

8.There should be defences against coercion and vote selling.

These abuses are equally possible with postal voting and there have been serious cases of this in the past. Voting in person, in the privacy of a voting booth, remains the best safeguard.

An online system that allows a voter to vote more than once and that only counts the final vote would provide some defence against coercion, because the voter could change their coerced vote later if they wished to do so.

Important Properties of an Online Voting System

9.The system should be secure against all forms of cyberattack.

Nation states have frequently sought to interfere in other countries' elections, so this must be viewed as a serious threat. The US Presidential election saw 120 fake Russian-backed pages create 80,000 posts that were received by 29 million Americans directly.

Twitter said that they had identified 50,248 Twitter accounts engaged in what it believed to be automated, election-related activity originating out of Russia.

The same Twitter accounts posted almost 45,000 messages about Brexit in the 48 hours around last year's referendum

Cybersecurity

- Cyberattacks are a Tier One threat on the National Risk Assessment

- In January 2018, Ciaran Martin, Head of the National Cybersecurity Centre said that *a major cyber-attack on the UK is a matter of "when, not if".*

- A report in the Guardian newspaper quoted him as saying ***"With the current state of high alert around elections, I think it make sense that there are not any current plans to move to electronic voting"***

- Cyberattacks could

  - influence opinion, disrupt voter registration, disrupt voting and undermine public confidence in the fairness of the result

  - target individual candidates or constituencies, particular religious or ethnic groups of voters, or the entire election

  - range from fake news stories and DDoS (distributed denial of service) attacks to penetration and compromise of online voting software and electronic counting.

Issues to Discuss

A. What is online voting meant to achieve?

- to increase voter participation;

- to provide voters with choice and flexibility over how they vote;

- to reduce the costs of elections;

- to reduce the number of rejected ballot papers;

- to increase the proportion of younger citizens who vote;

- to speed up the count so that the result can be announced sooner.

Issues to Discuss

B. What problems might online voting create - and would they be important?

- would there be more or less error, fraud or coercion?

- would voting become more casual and less of a considered opinion?

- would it become more or less of a secret ballot?

- would it be a good use of the money that it would cost to develop, assure and maintain the computer systems?

- can online voting ever be secure enough?

We use many online services.
What makes voting different?

"Voting is a uniquely difficult question for computer science: the system must verify your eligibility to vote; know whether you have already voted; and allow for audits and recounts. Yet it must always preserve your anonymity and privacy.

Currently, there are no practical solutions to this highly complex problem and existing systems are unacceptably flawed." Open Rights Group

Should We Vote Online?

Questions and Discussion

I look forward to hearing your views